

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-239129

(43)Date of publication of application : 31.08.1999

(51)Int.Cl.

H04L 9/32
G06F 12/14
G06F 13/00
G09C 1/00
G09C 5/00
H04N 1/387

(21)Application number : 10-106438

(71)Applicant : HITACHI LTD

(22)Date of filing : 16.04.1998

(72)Inventor : YOSHIURA YUTAKA
SUZAKI SEIICHI
TAKARAGI KAZUO
SASAKI RYOICHI
TOYOSHIMA HISASHI
SAITO TSUKASA

(30)Priority

Priority number : 09148061
09348860Priority date : 05.06.1997
18.12.1997

Priority country : JP

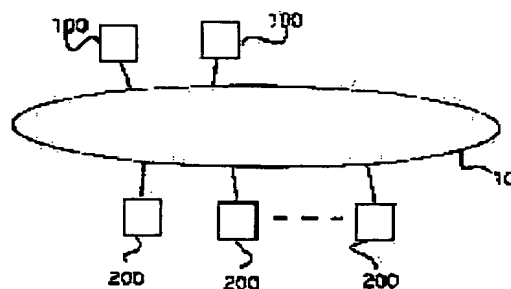
JP

(54) METHOD FOR CERTIFYING ELECTRONIC DATA

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for certifying electronic data by which the purchaser of the contents which become the original of an unauthorized copy can be specified with higher evidence.

SOLUTION: A provider device 100 sends the contents purchased by a purchaser to the device 200 of the purchaser after enciphering the contents by using the public key of the device 200 of the purchaser. The device 200 produces the electronic signature of the contents by using its own cryptographic key and buries the electronic signature in the sent contents in the form of an electronic watermark. Upon acquiring an unauthorized copy, the device 100 specifies the purchaser who has purchased the contents which become the original of the copy by verifying the electronic signature buried in the contents in the form of an electronic watermark.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-239129

(43) 公開日 平成11年(1999) 8月31日

(51) Int.Cl. ⁸	識別記号	F I	
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E
	3 5 4		3 5 4 D
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B
5/00		5/00	

審査請求 未請求 請求項の数19 O L (全 32 頁) 最終頁に続く

(21) 出願番号 特願平10-106438

(22) 出願日 平成10年(1998) 4月16日

(31) 優先権主張番号 特願平9-148061

(32) 優先日 平 9 (1997) 6 月 5 日

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平9-348860

(32) 優先日 平 9 (1997) 12 月 18 日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72) 発明者 吉浦 裕

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 宝木 和夫

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

最終頁に続く

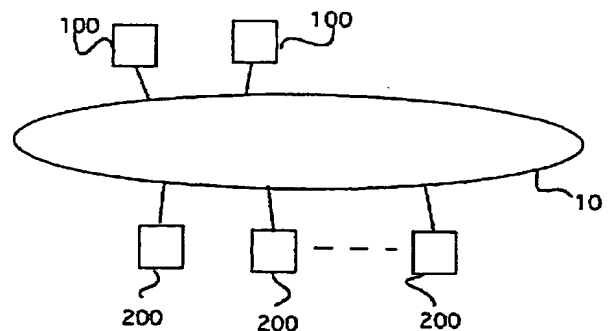
(54) 【発明の名称】 電子データを認証するための方法

(57) 【要約】

【課題】 不正コピーの元となったコンテンツを購入した購入者を、より高い証拠性をもって特定する。

【解決手段】 プロバイダー装置 100 は、購入者装置 200 の公開鍵を用いて、購入者が購入したコンテンツを暗号化して送付する。購入者装置 200 は、自身の秘密鍵を用いてコンテンツの電子署名を作成し、作成した電子署名を電子透かしとして送付されたコンテンツに埋め込む。不正コピーを入手した場合、プロバイダー装置 100 は、電子透かしの電子署名を検証し、この不正コピーの元となったコンテンツを購入した購入者を特定する。

図 1



【特許請求の範囲】

【請求項 1】電子計算機を用いて、コンテンツの埋め込み情報を処理するコンテンツ埋め込み情報の処理方法であって、

コンテンツの関係者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成するステップと、

作成した暗号情報を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込むステップと、

を有することを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 2】請求項 1 記載のコンテンツ埋め込み情報の処理方法であって、

暗号情報が埋め込まれたコンテンツから、暗号情報を抽出するステップと、

抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証するステップと、

を有することを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 3】請求項 1 記載のコンテンツ埋め込み情報の処理方法であって、

前記所定の情報を、前記暗号情報を埋め込むコンテンツの内容に依存した値をとる情報とすることにより、前記コンテンツの関係者の、当該コンテンツに対する電子署名を前記暗号情報としたことを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 4】請求項 1 記載のコンテンツ埋め込み情報の処理方法であって、

前記暗号情報の作成に先立ち、コンテンツの内容をハッシュ関数で評価し、評価した評価値であるハッシュ値を前記所定の情報として生成するステップを設けることにより、前記コンテンツの関係者の、当該コンテンツに対する電子署名を前記暗号情報としたことを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 5】電子計算機を用いて、コンテンツに、 k (k は 2 以上の整数) 人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、

第 1 番目のコンテンツ関係者の、公開鍵暗号体系に従った秘密鍵で、コンテンツを第 1 のハッシュ関数で評価した n ビットのハッシュ値を、暗号化した電子署名を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップと、

第 2 番目のコンテンツ関係者から第 k 番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者についての埋め込み処理を繰り返すステップとを有し、

第 i (ただし、 i は 2 以上 k 以下の整数) 番目のコンテンツ関係者についての前記埋め込み処理は、第 1 番目から第 $(i-1)$ 番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツを第 2 のハッシュ関数で評価した $n/2$ ビットのハッシュ値を、第 i 番目のコンテンツ関係者の秘密鍵で暗号化した電子署名を、第 1 番目から第 $(i-1)$ 番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込む処理であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 6】電子計算機を用いて、コンテンツに、 k (k は 2 以上の整数) 人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、

第 1 番目のコンテンツ関係者の公開鍵暗号体系に従った秘密鍵で、コンテンツを第 1 のハッシュ関数で評価したハッシュ値を暗号化した、当該第 1 番目のコンテンツ関係者の電子署名を作成するステップと、

第 2 番目のコンテンツ関係者から第 k 番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者について、当該コンテンツ関係者の電子署名を作成する電子署名作成処理を繰り返すステップと、

第 k 番目のコンテンツ作成者について実行された前記電子署名作成処理によって得られた第 k 番目のコンテンツ作成者の電子署名をコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップとを有し、

第 i (ただし、 i は 2 以上 k 以下の整数) 番目のコンテンツ関係者についての前記電子署名作成処理は、第 $(i-1)$ 番目のコンテンツ関係者の電子署名の値に依存して定まる値を、第 i 番目のコンテンツ関係者の秘密鍵で暗号化し、第 $i-1$ 番目のコンテンツ関係者の電子署名とする処理であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 7】請求項 6 記載のコンテンツ埋め込み情報の処理方法であって、

前記第 $(i-1)$ 番目のコンテンツ関係者の電子署名の値に依存して定まる値は、前記第 $(i-1)$ 番目のコンテンツ関係者の電子署名の値を、ハッシュ関数で評価したハッシュ値であることを特徴とするコンテンツ埋め込み情報の処理方法。

【請求項 8】情報開示者と情報閲覧者の双方が信頼する管理者によって管理されていて、かつ、真正性を確認可能なマルチメディアデータを、情報開示者は自己が公開する情報に対して付加し、情報閲覧者は該マルチメディアデータの真正性が確認されたかどうかに応じて前記情報の真正性を確認することを特徴とする情報の認証方法。

【請求項 9】少なくとも 1 つのクライアント端末と、前

記クライアント端末からの要求に応じて情報提供を行う少なくとも1つのWWWサーバと、前記クライアント端末やWWWサーバで使用されるマークを管理する少なくとも1つのマーク管理サーバと、が通信網を介して相互に接続されているシステムにおいてWWWサーバが公開するWebページを認証する方法であって、

前記WWWサーバが、自WWWサーバのURLデータを含むマーク送付要求を前記マーク管理サーバに送るステップと、

前記WWWサーバが、前記マーク管理サーバから返送されてきたマークを自己のWebページに貼り付けた後、該マークに前記マーク管理サーバへのリンク情報を設定し、前記クライアント端末からアクセス可能な状態で該マーク付きWebページを公開するステップと、

前記マーク管理サーバが、自マーク管理サーバの管理対象であるマークの送付状況などをマーク管理DBに記憶するステップと、

前記マーク管理サーバが、前記WWWサーバからのマーク送付要求を受け取った場合に、該WWWサーバがマークを取得する条件を満たしているかどうかを判定し、条件を満たしていると判定した場合にのみ、前記マーク管理DBを更新してから、前記要求のあったマークを当該WWWサーバに返送するステップと、

前記マーク管理サーバが、前記クライアント端末からの真正性確認要求を受け取った場合に、前記マーク管理DBを参照して該要求のあったマークの真正性を検証し、該検証結果を当該クライアント端末に返送するステップと、

前記クライアント端末が、前記WWWサーバから前記マーク付きWebページをダウンロードするステップと、前記クライアント端末が、前記ダウンロードしたマーク付きWebページのURLデータを含む真正性確認要求をマーク管理サーバに送り、当該検証結果を受け取るステップとを備えていることを特徴とする方法。

【請求項10】少なくとも1つのクライアント端末と、前記クライアント端末からの要求に応じて情報提供を行う少なくとも1つのWWWサーバと、前記クライアント端末やWWWサーバで使用されるマークを管理する少なくとも1つのマーク管理サーバと、が通信網を介して相互に接続されているシステムにおいてWWWサーバが公開するWebページを認証する方法であって、

前記WWWサーバが、自WWWサーバのURLデータを含むマーク送付要求を前記マーク管理サーバに送るステップと、

前記WWWサーバが、前記マーク管理サーバから返送されてきた署名付きマークを自己のWebページに貼り付けた後、前記クライアント端末からアクセス可能な状態で該マーク付きWebページを公開するステップと、

前記マーク管理サーバが、自マーク管理サーバの管理対象であるマークの送付状況などをマーク管理DBに記憶

するステップと、

前記マーク管理サーバが、前記クライアント端末からの公開鍵送付要求を受け取った場合に、自マーク管理サーバの公開鍵を当該クライアント端末に返送するステップと、

前記マーク管理サーバが、前記WWWサーバからのマーク送付要求を受け取った場合に、該WWWサーバがマークを取得する条件を満たしているかどうかを判定し、条件を満たしていると判定した場合にのみ、前記マーク管理DBを更新してから、前記要求に含まれる前記WWWサーバのURLデータに電子的な署名を施し、要求のあったマークと該署名とを一纏めにして署名付きマークを生成して当該WWWサーバに返送するステップと、

前記クライアント端末が、公開鍵送付要求を前記マーク管理サーバに送るステップと、

前記クライアント端末が、前記マーク管理サーバから返送されてきた該マーク管理サーバ公開鍵を、公開鍵DBに記憶するステップと、

前記クライアント端末が、前記WWWサーバから前記マーク付きWebページをダウンロードするステップと、前記クライアント端末が、前記公開鍵DBを参照して、前記ダウンロードしたマーク付きWebページに含まれる署名を検証するステップとを有することを特徴とする方法。

【請求項11】請求項10記載の方法であって、署名付きマークを生成する場合に、前記WWWサーバのURLデータに加えて、マークとして用いている画像データも署名対象とし、該マークと署名とから署名付きマークを生成することを特徴とする方法。

【請求項12】請求項10記載の方法であって、署名付きマークを生成する場合に、さらに、前記Webページも署名対象とし、該マークと署名とから署名付きマークを生成することを特徴とする方法。

【請求項13】請求項10記載の方法であって、署名付きマークを生成する場合に、マークと署名とだけでなく、本システムに関連した何らかの属性情報も署名付きマークの構成要素の一つとすることを特徴とする方法を特徴とする方法。

【請求項14】電子計算機を用いて、電子データに当該電子データを認証するための認証用データを含めた認証可能電子データを作成する方法であって、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、

生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップとを有することを特徴とする方法。

【請求項15】請求項14記載の方法であって、

前記所定の情報は、前記電子データを所定のハッシュ関数で評価したハッシュ値であることを特徴とする方法。

【請求項 16】請求項 14 記載の方法であって、前記所定の情報は、前記電子データを所定の関数で評価した評価値を、所定の公開鍵暗号法に従った秘密鍵で暗号化した電子署名であることを特徴とする方法。

【請求項 17】請求項 14 記載の方法であって、前記認証可能電子データから前記マーク用データを切り出すステップと、切り出した前記マーク用データから電子透かしとして埋め込まれた前記所定の情報を抽出するステップと、抽出した情報に基づいて電子データを認証するステップとを有することを特徴とする方法。

【請求項 18】請求項 15 記載の方法であって、前記認証可能電子データから前記マーク用データを切り出すステップと、切り出した前記マーク用データから電子透かしとして埋め込まれたハッシュ値を抽出するステップと、前記認証可能電子データに基づいて、前記電子データを前記所定のハッシュ関数で評価したハッシュ値を算出するステップと、抽出したハッシュ値と算出したハッシュ値が一致した場合に、電子データの認証が成功したと判定するステップとを有することを特徴とする方法。

【請求項 19】請求項 16 記載の方法であって、前記認証可能電子データから前記マーク用データを切り出すステップと、切り出した前記マーク用データから電子透かしとして埋め込まれた電子署名を抽出するステップと、抽出した電子署名を前記秘密鍵に対応する公開鍵で復号化して得られる評価値を抽出する手段と、前記認証可能電子データに基づいて、前記電子データを前記所定の関数で評価した評価値を算出するステップと、抽出したハッシュ値と算出したハッシュ値が一致した場合に、電子データの認証が成功したと判定するステップとを有することを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子データと個人／機関との関係を認証可能とする技術に関するものである。

【0002】

【従来の技術】近年の情報化社会の発展に伴い、電子データが、従来の伝統的な印刷物に代わって、各種情報の伝達媒体として利用されることが増えている。また、電子データ自身が、価値ある商品として商取引の対象となることもある。

【0003】このような情報化社会では、電子データの不正な複製や改竄や使用による犯罪や、悪意ある行為を

防ぐために、電子データと個人／機関との関係を認証可能とすることが必要となる。たとえば、電子データが何かしらの権限ある機関により保証されたものであるかどうかを確認できるようにするためには、その電子データと権限ある機関との関係が認証可能である必要がある。同様に、電子データの出所や電子データに対して保有する個人や機関の権利などを確認するためには、その電子データと個人や機関との関係が認証可能である必要がある。

【0004】従来、電子データと個人／機関との関係を認証可能とする技術としては、電子署名と呼ばれる技術が知られている。

【0005】電子署名は、暗号理論入門、共立出版（1993年）133頁～137頁などに記載されているように、書類の真正さを保証するための技術であり、公開鍵暗号技術と一方向性関数を組み合わせたものである。

【0006】この技術では、まず、 $g(f(n, S), V) = n$ 、 $f(g(n, V), S) = n$ が成立する秘密鍵 S 、公開鍵 V の組を作成する。ここで n は任意のデータ、 f 、 g は所定の関数であり、上記式は、秘密鍵 S を用いて暗号化した任意のデータは公開鍵 V を用いて復号化することができ、また、逆に、公開鍵 V を用いて暗号化した任意のデータは秘密鍵 S で復号化できることを表している。また、ここで、公開鍵 V から秘密鍵 S を求めることは実質的に不可能となっている。

【0007】秘密鍵 S 、公開鍵 V を作成したならば、作成者は公開鍵 V を、相手方に渡し、秘密鍵 S は作成者が秘密に保持する。

【0008】そして、鍵の作成者が、相手方にデータを送る場合には、データを所定の一方関数で評価した評価値を秘密鍵 S で暗号化した電子署名をデータに添付して相手方に渡す。

【0009】ここで、一方関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に実用上不可能である性質をもつ。また、この電子署名で用いる一方関数には、実質的に異なるデータに対して異なるビット列を返す関数であること、すなわち、異なるデータに対して同じビット列を返す確率が極めて低い関数であること必要となる。このような関数としては、データの評価値として所定のビット列を返す一方ハッシュ関数などが知られている。ここで一方ハッシュ関数を、 h で表した場合の、データ D の一方ハッシュ関数による評価値 $h(D)$ を D のハッシュ値と呼ぶ。

【0010】さて、電子署名が添付されたデータを受け取った相手方は、データを一方関数で評価して評価値を求め、この評価値が、電子署名を公開鍵 V を用いて復号化した値と一致するかを検証する。そして、一致した場合には、電子署名が公開鍵 V に対応する秘密鍵 S の保持者によって成されたものであり、かつ、その電子署名

の対象が受け取ったデータであることを認証する。

【0011】また、一つのデータに対して複数人の電子署名を行う技術として、Applied Cryptography, Jhon W. Ily & Sons, Inc. (1996), pp 39-41に記載の技術が知られている。

【0012】この技術は、各自がデータのハッシュ値を電子署名として用いるのではなく、第2番目以降の署名者は、前の署名者の電子署名のハッシュ値を自身の電子署名として用いるものである。すなわち、第1番目の署名者は、上述したのと同様にデータのハッシュ値を自身の秘密鍵で暗号化し電子署名とする。そして、第2番目の署名者は第1番目の署名者の電子署名のハッシュ値を自身の秘密鍵で暗号化し自身の電子署名とする。以降、同様に、第n番目の署名者は、前の署名者の電子署名のハッシュ値を、第n番目の秘密鍵で暗号化して、第n番目の署名者の電子署名とする。

【0013】この場合、n人の署名者によって成された電子署名の検証は、次のように行う。すなわち、電子署名を、第n番目の署名者の公開鍵で復号化し、復号した電子署名を第n-1番目の署名者の公開鍵で復号化するといったように、順次、復号化し、第1番目の公開鍵で復号化した結果が、データのハッシュ値と一致すれば、この電子署名は、各公開鍵の所有者であるn人の署名者によって、当該データに対して成されたものであるとする。ただし、署名者の署名の順序が分からない場合などには、全ての署名者の順列について検証する必要が生じる。

【0014】また、従来、電子データを、個人／機関との関係において認証可能とする技術としては、電子透かし(digital watermark)と呼ばれる技術が知られている。

【0015】この技術は、日経エレクトロニクス(1997年)683号99頁から107頁などに記載されているように、イメージデータの著作権などの管理情報を、イメージデータ自体にイメージデータと不可分に埋め込む技術である。

【0016】この電子透かしの技術は、次のような特徴を持っている。すなわち、埋め込まれた情報は、情報を埋め込んだイメージデータを表示した場合にも一般的には視認されず、また、視認可能な範囲において画像自体をほとんど変化させない。一方、埋め込まれた情報のみを正確に除去することは容易でない反面、不正確に除去すると画像の画質が著しく劣化する。また、一般的には、ある程度までは、イメージデータを圧縮した場合にも、埋め込んだ情報を復元することができる。

【0017】この他、電子透かしの技術としては、イメージデータを対象とするのではなく、テキストやドローデータ(図面データ)やオーディオデータを対象とするものなどが提案されている。

【0018】なお、日経エレクトロニクス(1997年)6

83号99頁から107頁には、このような電子透かしを利用して、イメージデータなどの電子データであるコンテンツの不正コピーを防止する技術も記載されている。

【0019】この技術は、コンテンツに、コンテンツを購入した者の識別情報を電子透かしとして埋め込み、不正コピーされたコンテンツが押収されたときには、これに埋め込まれた情報を抽出し、不正コピーを行った者(すなわち購入者)を特定するものである。

【0020】ここで、このような購入者の識別情報のコンテンツへの埋め込みは、基本的には以下の手順で行われる。

【0021】(1)購入者がコンテンツの購入を希望したら、プロバイダー(コンテンツの提供者)はその購入者にユニークな番号を割り当てる。

【0022】(2)プロバイダーは、コンテンツに、そのコンテンツの購入者の番号を電子透かしとして埋め込む。

【0023】(3)不正コピーされたコンテンツをプロバイダーまたは監査機関が押収したときに、そのコンテンツから購入者の番号を抽出し、購入者を特定する。

【0024】(4)購入者がコンテンツの不正コピーを行った、あるいは、不正コピー者にコンテンツを手渡したとして、購入者にペナルティを科す。

【0025】ところで、近年の、インターネットのようなオープンなネットワークを使って、複数のユーザに情報を開示・伝達する手段として、World Wide Web(WWW)サーバプログラムとブラウザプログラムとを用いるWWWシステムの普及や利用範囲の拡大に伴い、WWWサーバ上で公開される電子データであるwebページについても、WWWシステムの不正な使用による犯罪や、悪意ある行為を防ぐために、webページを、個人／機関との関係において認証可能とすることが必要となる。たとえば、webページ上で何かしらの権限ある機関により保証されたものであることが提示されている場合に、真に、そのwebページが権限ある機関により保証されたものであることを確認できるようにするためには、そのwebページが権限ある機関との関係において認証可能である必要がある。同様に、webページの発信者やwebページに対して保有する個人や機関の権利などを確認するためには、そのwebページが個人や機関との関係において認証可能である必要がある。

【0026】なお、たとえば「OPEN DESIGN 96年4月号」(発行人：蒲生良治、発行所：CQ出版株式会社)の4ページから22ページおよび40ページから78ページに記載されているように、WWWシステムは、操作性に優れたグラフィカルユーザインタフェース(GUI)を備えているとともに、関連性のある様々な情報をハイパーリンクでつなぐことで簡単に参照できるようにすることができるなどユーザの利便性にも優れており、今日のこれほどまで急速なインターネットの

発展は、このWWWシステムによるところが大である。

【0027】この文献に記載されたWWWシステムの概要を簡単に説明する。

【0028】WWWシステムは、情報を公開するためのWWWサーバプログラムが動作する少なくとも一つのWWWサーバと、当該公開情報を閲覧するためのブラウザプログラムが動作する少なくとも一つのクライアント端末からなり、WWWサーバとクライアント端末との間は、HTTP(HyperText Transfer Protocol)と呼ばれる通信プロトコルによりデータのやり取りが行われる。

【0029】WWWサーバで情報を公開する場合、まず、当該サーバに格納された公開すべきテキストデータ、イメージデータ、オーディオデータ、ビデオデータ、あるいは他Webページへのハイパーリンクデータなどを、HTML(Hyper Text Markup Language)と呼ばれる構造化記述言語を用いて相互に関連付けて一纏めにしたWebページを作成する。次に、このWebページを、他のコンピュータ(クライアント端末や他のWWWサーバ)からアクセス可能な状態で、WWWサーバの任意の格納場所(ディレクトリ)に保管する。

【0030】一方、公開されたWebページを、ユーザがクライアント端末からブラウザプログラムを用いて閲覧する場合、クライアント端末を利用するユーザがブラウザプログラムに対して、上記WebページのURL(Universal Resource Locator)を指定すると、そのWebページのデータがWWWサーバよりクライアント端末に送られる。そして、そのWebページに含まれるテキストデータ、イメージデータ、ビデオデータなどがクライアント端末の画面上に表示される。また、オーディオデータは当該クライアント端末に接続されたスピーカなどから出力される。

【0031】ところで、近年では、このようなWWWシステムを単なる情報伝達手段としてだけでなく、ビジネスに利用しようという動きが顕著である。たとえば、WWWシステムにより商品情報を公開するいわゆる電子商取引システムなどはそのようなビジネス利用の代表例である。

【0032】このような電子商取引システムの概要については、たとえば「情報処理 第38巻 第9号」(発行人：飯塚 浩司、発行所：社団法人 情報処理学会)の752ページから810ページに記載されている。

【0033】この文献では、上記電子商取引システムを、単なる商品情報を消費者に開示するためのシステムではなく、共通鍵暗号や公開鍵暗号といった暗号技術や、デジタル署名などの認証技術を駆使し、決済までも行うシステムとして提示している。また、この場合における決済方法としては銀行決済やクレジット決済、あるいは電子マネーによる決済などいろいろな方法を取

ることを想定している。

【0034】このような電子商取引システムでは、販売者は、自己のWebページに利用可能なクレジットカード会社のロゴマークなどのイメージデータを含め、消費者が支払方法を一目で認識できるようにすることが多い。これは、現実世界(インターネットのようなバーチャルな世界ではない)において、各販売店(クレジットカード会社の加盟店)に、そこで使用可能なクレジットカードのロゴマークが掲示されていると同様である。

【0035】また、この他、Webページの発信者を示すロゴマークや、そのwebページを承認した何らかの権限ある個人/機関を示すロゴマークなどのイメージデータをWebページに含め、webページの利用者が、一目で、webページの発信者やwebページが権限ある個人/機関に承認されていることを認識できるようにすることもある。

【0036】

【発明が解決しようとする課題】前記、電子透かしの技術によれば、次のような問題がある。

【0037】まず、第1に、電子透かしとして埋め込まれた情報と、当該情報が提示する個人/機関との関係が保証されない。すなわち、電子データに埋め込まれた情報が、個人/機関と電子データ関係を正しく表していることを保証できない。

【0038】このため、たとえば、前述した不正コピーを防止する技術では、不正コピーコンテンツに埋め込まれた番号が、真に不正コピーされたコンテンツを購入した者を示す番号であるという証拠となりにくい。すなわち、プロバイダーが購入者に一方的に与える番号であるため、購入者は、番号と自身との対応を否認できる可能性がある。

【0039】また、前述したwebページの場合は、不正者が、他人を示す情報を偽造して電子透かしとして埋め込んで、他人を装ったり、権限ある機関に保証されていることを装う可能性を否定できない。

【0040】第2に、電子データと、電子透かしとして埋め込まれた情報が示す個人/機関との関係が保証されない。

【0041】このため、たとえば、前述した不正コピーを防止する技術では、購入者の番号が、購入者が買ったコンテンツに正しく埋め込まれたという証拠がない。すなわち、購入者が買っていないコンテンツに、購入者以外(例えばプロバイダーの内部者)が誤って、もしくは、不正目的で購入者番号を埋め込んだ可能性を否定できない。

【0042】また、前述したwebページの場合は、個人/機関が正規のwebページに対して埋め込んだ電子透かしを抽出し、不正目的で作成したwebページに対して電子透かしとして埋め込んで、他人を装ったり、権限ある機関に保証されていることを装う可能性を否定できな

い。

【0043】また、第3に、電子透かしの技術によって、コンテンツに著作権の情報を埋め込む技術によれば、一つのコンテンツに対して多数の権利者が存在した場合、埋め込むべき情報量が多くなりコンテンツの質（例えば、コンテンツが画像である場合は画質）を大きく劣化させてしまう。また、第4に、電子透かしの技術は、webページのような複数種のデータを含む電子データに適していない。たとえば、テキスト、ドローデータ（図面データ）、イメージデータを含む電子データに適用するためには、データの種類毎に異なった処理を行わなければならない。

【0044】一方、前記電子署名の技術によれば、電子データに他に、電子署名を電子データと組で管理しなければならないという煩わしさがある。また、電子署名は、電子透かしに比べ電子データと分離することが極めて容易であるため、前述した不正コピーの防止の目的のために用いることができない。

【0045】また、前記電子透かし、電子署名の技術とも、不可視であるため、電子透かし、電子署名が示す電子データと個人／機関との関係を、電子データの利用者に直接提示することができないという問題もある。

【0046】たとえば、電子透かし、電子署名では、前述したロゴマークをイメージデータとして含めたwebページのように、一目でwebページと個人／機関との関係を利用者に提示することができない。また、このことは、電子透かし、電子署名が示す電子データと個人／機関との関係と、電子データが利用者に直接示す電子データと個人／機関との関係が一致していることが電子透かし、電子署名によっては直接保証されないことを意味する。

【0047】一方、Webページ上にロゴマークをイメージデータとして含める技術によれば、ロゴマークが単なるイメージデータであるため、ロゴマークが示す個人／機関との関係をWebページが真に有しているのかどうかを認証することができない。

【0048】このため、たとえば、前記クレジット会社のロゴマークを例にとれば、不正者が、当該クレジットカード会社の正規加盟店のWebページから当該ロゴマークをコピーし、自己の販売店のWebページの適当な個所に該ロゴマークを貼り付けてから、該Webページを他のコンピュータからアクセス可能な状態で、WWWサーバの任意の格納場所に保管した場合、消費者は、不正者のWebページに含まれる上記クレジットカード会社のロゴマークを見て、その不正者が正規の加盟店であるものと判断し、自己のクレジットカード番号など決済に必要なデータを当該WWWサーバに送信してしまう可能性がある。結果、不正者は、入手した消費者のクレジット番号を不正に入手し不正な利益を得ることが可能となる。

【0049】そこで、本発明は、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする技術を提供することを課題とする。また、電子データとの関係を認証可能な個人／機関と一致することが保証されるように、電子データと関係を持つ個人／機関を電子データによって利用者に直接提示ことを課題とする。

【0050】

【課題を解決するための手段】前記課題達成のために、本発明は、たとえば、電子計算機を用いて、コンテンツの埋め込み情報を処理するコンテンツ埋め込み情報の処理方法であって、コンテンツの関係者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成するステップと、作成した暗号情報を、コンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込むステップとを有することを特徴とするコンテンツ埋め込み情報の処理方法を提供する。

【0051】ただし、ここで、少なくとも所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないとは、所定の規則を用いない場合には、試行錯誤的な処理以外の処理で分離することができないことを意味する。

【0052】このような方法によれば、暗号情報が埋め込まれたコンテンツから、暗号情報を抽出し、抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証することにより、暗号情報が埋め込まれたコンテンツが不正コピーである場合に、当該不正コピーの元となったコンテンツの関係者を特定することができる。

【0053】そして、この場合において、このような判断は、不正コピーに埋め込まれた、個々のコンテンツ関係者自身しか知らないことが保証されるコンテンツ関係者の秘密鍵に依存し、したがって購入者自身しか作成することのできない情報の検証によって行われるので、不正コピーに埋め込まれた情報と、不正コピーの起因となったコンテンツ関係者との対応の証拠性を向上することができる。

【0054】また、埋め込む暗号情報を、暗号情報を埋め込むコンテンツの内容に依存した値をとる、たとえば、コンテンツのハッシュ値を秘密鍵で暗号化した電子署名とすれば、不正コピーに埋め込まれた情報が示すコンテンツ関係者のとコンテンツとの対応性の証拠性も向上することができる。

【0055】また、本発明は、前記課題達成のために、電子計算機を用いて、コンテンツに、 k (k は2以上の整数)人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、第1番目のコンテンツ関係者の、公開鍵暗号体系に従った秘密鍵で、コンテンツを第1のハッシュ関数で評価した n ビットのハッシュ値を、暗号化した電子署名を、コンテンツに、所定

の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップと、第 2 番目のコンテンツ関係者から第 k 番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者についての埋め込み処理を繰り返すステップとを有し、第 i (ただし、 i は 2 以上 k 以下の整数) 番目のコンテンツ関係者についての前記埋め込み処理は、第 1 番目から第 $(i-1)$ 番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツを第 2 のハッシュ関数で評価した $n/2$ ビットのハッシュ値を、第 i 番目のコンテンツ関係者の秘密鍵で暗号化した電子署名を、第 1 番目から第 $(i-1)$ 番目までのコンテンツ関係者の電子署名が埋め込まれたコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込む処理であることを特徴とするコンテンツ埋め込み情報の処理方法を提供する。

【0056】この方法によれば、 k 人の電子署名のコンテンツの埋め込みを、 $n + (k-1) \times n/2$ ビットのデータの埋め込みで達成できる。また、後述するように、そのセキュリティを大きく劣化することもない。

【0057】また、本発明が提供する電子計算機を用いて、コンテンツに、 k (k は 2 以上の整数) 人のコンテンツ関係者の情報を埋め込むコンテンツ埋め込み情報の処理方法であって、第 1 番目のコンテンツ関係者の公開鍵暗号体系に従った秘密鍵で、コンテンツを第 1 のハッシュ関数で評価したハッシュ値を暗号化した、当該第 1 番目のコンテンツ関係者の電子署名を作成するステップと、第 2 番目のコンテンツ関係者から第 k 番目のコンテンツ関係者まで、順次、当該順番に従って、各コンテンツ関係者について、当該コンテンツ関係者の電子署名を作成する電子署名作成処理を繰り返すステップと、第 k 番目のコンテンツ作成者について実行された前記電子署名作成処理によって得られた第 k 番目のコンテンツ作成者の電子署名をコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該電子署名のみを当該コンテンツから分離できないように埋め込むステップとを有し、第 i (ただし、 i は 2 以上 k 以下の整数) 番目のコンテンツ関係者についての前記電子署名作成処理は、第 $(i-1)$ 番目のコンテンツ関係者の電子署名の値に依存して定まる値を、第 i 番目のコンテンツ関係者の秘密鍵で暗号化し、第 $i-1$ 番目のコンテンツ関係者の電子署名とする処理であることを特徴とするコンテンツ埋め込み情報の処理方法によれば、電子署名の値に依存して定まる値を n ビットとすれば、 n ビットのデータをコンテンツに埋め込むだけで、 k 人のコンテンツ関係者を検証できる情報をコンテンツに埋め込むことができる。

【0058】また、前記課題を達成するために、本発明は、たとえば、情報開示者と情報閲覧者の双方が信頼する管理者によって管理されていて、真正性を確認可能な

マルチメディアデータを、情報開示者は自己が公開する情報に対して付加し、情報閲覧者は該マルチメディアデータの真正性が確認されたかどうかに応じて前記情報の真正性を確認することを特徴とする情報の認証方法。を提供する。

【0059】このような方法では、情報の真正性は、たとえば、情報に付加されたマルチメディアデータに対する、全ての関与者が信頼する管理者の真正性の確認に応じて判定される。

【0060】具体的には、たとえば、Web ページを閲覧するユーザが、その Web ページに貼り付けられた画像データが明示する情報 (ユーザが見た目から判断するであろう情報) が真正なものであるか否か、すなわち、画像データ自体が本物であるか否か、さらには、その Web ページに当該画像データを貼り付けているという事実が、前記画像データが明示する該画像データの管理者に認められたものであるか否かを管理者が認証するか否かに応じて、Web ページの真正性を判定する。

【0061】なお、このような方法において、必要に応じて、上記マルチメディアデータの真正性が確認された場合に上記情報閲覧者に対して当該情報を提供するようにしてもよい。具体的には、たとえば、前記 Web ページ例では、上記画像データが真正なものであると確認された場合に、当該 Web ページを表示するように、情報をフィルタリングするようにしてもよい。

【0062】また、前記課題達成のために本発明は、電子計算機を用いて、電子データに当該電子データを認証するための認証用データを含めた認証可能電子データを作成する方法であって、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップとを有することを特徴とする方法を提供する。

【0063】ここで、このような方法において、前記所定の情報は、前記電子データを所定のハッシュ関数で評価したハッシュ値であってもよい。

【0064】また、前記所定の情報は、前記電子データを所定の関数で評価した評価値を、所定の公開鍵暗号法に従った秘密鍵で暗号化した電子署名であってもよい。

【0065】これらのような方法によれば、透かし入りマーク用データに電子透かしとして埋め込まれた情報より、そのマークの真正性を認証可能となる。また、さらに、ハッシュ値を電子透かしとして埋め込む場合は、そのマークがその電子データに対して与えられたことを認証することができる。また、さらに、電子署名を電子透かしとして埋め込む場合には、さらに、そのマークを保証する個人/機関をも認証することができるようにな

る。

【0066】また、本発明は、この他、前記各方法を実現するためのシステムや装置を提供する。

【0067】例を挙げれば、たとえば、配布するコンテンツを出力する配布側装置と、配布されたコンテンツを入力する受領側装置とを有するコンテンツ配布システムであって、配布側装置は、配布するコンテンツを暗号化する暗号化手段を備え、受領側装置は、配布されたコンテンツを復号化する復号化手段と、受領側装置の利用者の、公開鍵暗号体系に従った秘密鍵で、所定の情報を暗号化した暗号情報を作成する署名作成手段と、作成した暗号情報を、復号化したコンテンツに、所定の規則に従って、少なくとも当該所定の規則を用いずに当該暗号情報のみを当該コンテンツから分離できないように埋め込む署名埋め込み手段と、を有することを特徴とするコンテンツ配布システムを提供する。

【0068】また、このようなコンテンツ配布システムであって、署名作成手段が行う暗号情報の作成および前記署名埋め込み手段の行う暗号情報の埋め込みとを行わずに、前記復号化手段の復号化のみを行うことができないように前記復号化手段と署名作成手段と署名埋め込み手段とは構成されており、かつ、署名作成手段が行う暗号情報の作成および前記署名埋め込み手段の行う暗号情報の埋め込みとを行わずに、前記復号化手段の復号化のみを行うように改変することを困難化するプロテクトが受領側装置に設けられていることを特徴とするコンテンツ配布システムを提供する。

【0069】また、さらには、これらのコンテンツ配布システムであって、前記配布側装置の暗号化手段は、受領側装置の利用者の公開鍵を用いてコンテンツを暗号化し、前記受領側装置の復号化手段は、配布側装置の利用者の秘密鍵を用いて暗号化されたコンテンツを復号化することを特徴とするコンテンツ配布システムを提供する。

【0070】なお、これらのコンテンツ配布システムに検証装置を備え、当該検証装置は、暗号情報が埋め込まれたコンテンツから、暗号情報を抽出する署名抽出手段と、抽出した暗号情報を、コンテンツの関係者の公開鍵で復号化した結果が、前記所定の情報と一致するかを検証する署名検証手段と、を有するようにしてもよい。

【0071】また、これらのコンテンツ配布システムにおいては、受領側装置の署名作成手段は、復号化したコンテンツの内容に依存した値をとる情報を前記所定の情報とし、当該所定の情報を、受領側装置の利用者の、公開鍵暗号体系に従った秘密鍵で暗号化した、当該利用者の当該コンテンツに対する電子署名を、前記暗号情報として作成するようにしてもよい。

【0072】また、本発明は、たとえば、コンテンツに署名を施すデータ処理装置であって、コンテンツをハッシュ関数で評価したハッシュ値を算出し、算出したハッ

シュ値を、当該データ処理装置の利用者の、公開鍵暗号体系に従った秘密鍵で暗号化し、電子署名とする電子署名作成手段と、作成した電子署名を電子透かしとして、コンテンツに埋め込む電子透かし作成手段とを有することを特徴とするデータ処理装置を提供する。

【0073】また、本発明は、たとえば、認証可能電子データを生成する生成側装置と、認証可能電子データの認証する認証側装置から構成されるシステムであって、生成側装置は、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成する手段と、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成する手段と、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成する手段とを有し、前記認証側装置は、前記認証可能電子データから前記マーク用データを切り出す手段と、切り出した前記マーク用データから電子透かしとして埋め込まれた前記所定の情報を抽出する手段と、抽出した情報に基づいて電子データを認証する手段とを有するシステムを提供する。

【0074】より具体的には、たとえば、前記認証可能電子データは、マーク用データを含んだwebページであり、前記認証側装置では、当該webページ及び、当該webページ閲覧時にマーク用データによって出力される内容が示す事項の認証を、マーク用データに電子透かしとして埋め込まれた情報に基づいて行う。なお、この場合、前記認証可能電子データであるwebページを生成する装置／機関と、このwebページを公開する装置／機関は異なる装置であってよい。また、この場合、webページを公開する装置／機関よりの依頼に応じて、前記認証可能電子データであるwebページを生成する装置／機関が前記認証可能電子データであるwebページを作成するようにしてよい。

【0075】また、本発明は、前記各方法を電子計算機に実施させるためのプログラムを記憶した記憶媒体をも提供する。

【0076】例を挙げれば、たとえば、電子計算機によって実行されるプログラムを記憶した、電子計算機読み取り可能な記憶媒体であって、前記プログラムは、電子データの利用時に利用者が認知可能な出力を行うマーク用データを生成するステップと、前記マーク用データに所定の情報を電子透かしとして埋め込んだ、透かし入りマーク用データを生成するステップと、生成した透かし入りマーク用データを、前記電子データに含め、前記認証可能電子データを生成するステップと、を電子計算機に実行させるプログラムであることを特徴とする記憶媒体を提供する。

【0077】また、たとえば、電子計算機によって実行されるプログラムを記憶した、電子計算機読み取り可能な記憶媒体であって、前記プログラムは、

【0078】

【発明の実施の形態】以下、本発明の実施形態について説明する。

【0079】まず、復号的でない電子データについて、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする実施形態を、第1、第2、第3実施形態として説明する。

【0080】まず、第1の実施形態について説明する。

【0081】本第1実施形態では、電子データと個人／機関との関係を認証可能とする例として、電子データであるコンテンツの不正コピーを防止する目的のために、コンテンツとコンテンツの購入者との関係を認証可能とする場合を例にとり説明する。ただし、電子データと個人／機関との関係を認証可能とする目的に応じて、本第1実施形態は、電子データとの関係を認証可能とする個人／機関を、コンテンツの購入者ではなく、コンテンツの権利者、コンテンツの販売者、コンテンツを取り扱う中間業者などとするように修正してよい。また、本第1実施形態および後述する第2、第3実施形態では、コンテンツがイメージデータである場合を例にとるが、これは、コンテンツが他の種類のデータ、たとえば、テキストデータやドローイングデータやオウディオデータやビデオデータであるように修正してよい。

【0082】まず、本実施形態に係るコンテンツ配布システムの構成を図1に示す。

【0083】図示するように、コンテンツ配布システムは電子データであるコンテンツを配布するプロバイダー装置100と、コンテンツの配布を受ける通常複数の購入者装置200より構成される。

【0084】プロバイダー装置100と購入者装置200の間のコンテンツや、その他の情報のやりとりは、プロバイダー装置100と購入者装置200を結ぶネットワーク10を介して行われる。ただし、ネットワーク10は必ずしも必要ではなく、プロバイダー装置100と購入者装置200の間のコンテンツや、その他の情報のやりとりは、当該情報を記憶したフロッピーディスクなどの記憶媒体の運送、郵送などによってもよい。

【0085】図2に、プロバイダー装置100と購入者装置200の構成を示す。

【0086】図示するように、プロバイダー装置100は、処理部110と記憶部120よりなり、処理部110は、入出力を担う入出力部111、プロバイダー装置100内の各部の制御を行う制御部112、電子署名が埋め込まれたコンテンツから電子署名を抽出する署名抽出部113、電子署名を検証する署名検証部114、コンテンツを暗号化する暗号化部115、各購入者装置200との間の送受信を担う送受信部116よりなる。また、記憶部120は、コンテンツ121や検証鍵122を記憶する。ここで、検証鍵122が、従来の技術の欄で説明した公開鍵に相当する。

【0087】また、図示するように、購入者装置200

は、処理部210と記憶部220よりなる。また、処理部210は、入出力を担う入出力部211、購入者装置200内の各部の制御を行う制御部212、プロバイダー装置100との間の送受信を担う送受信部213、暗号化されたコンテンツの復号を行う復号化部214、電子署名を作成する署名生成部215、電子署名をコンテンツに埋め込む署名埋め込み部216、署名鍵（秘密鍵）と検証鍵（公開鍵）を作成する鍵生成部217よりなる。また、記憶部220は、電署名鍵221や署名入りコンテンツ222を記憶する。ここで署名鍵221が、従来の技術の欄で説明した秘密鍵に相当する。

【0088】ここで、プロバイダー装置100や購入者装置200は、図3に示すように、CPU301や、主記憶302、ハードディスク装置である外部記憶装置303b、他の外部記憶装置である303a、通信制御装置304、キーボードやポインティングデバイスなどの入力装置305、表示装置などの出力装置306などを備えた、一般的な構成を有する電子計算機上に構築することができる。

【0089】この場合、プロバイダー装置100の処理部110、および、処理部110の内部の各部は、CPU301が主記憶302にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶302や外部記憶装置303a、bが、プロバイダー装置100の記憶部120として使用される。また、同様に、購入者装置200の処理部210、および、処理部210の内部の各部は、CPU301が主記憶302にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶302や外部記憶装置303が、購入者装置200の記憶部220として使用される。

【0090】前述した主記憶302にロードされCPU301によって実行されることにより、電子計算機上にプロバイダー装置100と購入者装置200を構成するためのプログラムは、予め、外部記憶装置303bに記憶され、必要に応じて主記憶302にロードされ、CPU301によって実行される。または、可搬型の記憶媒体307、たとえば、CD-ROMを扱う外部記憶装置303aを介して、直接、必要に応じて、可搬型の記憶媒体307から主記憶302にロードされ、CPU301によって実行される。もしくは、一旦、可搬型の記憶媒体を扱う外部記憶装置303aを介して、可搬型の記憶媒体307から、ハードディスク装置などの外部記憶装置303b上にインストールされた後、必要に応じて主記憶302にロードされ、CPU301によって実行される。

【0091】以下、プロバイダー装置100と購入者装置200の行う処理の詳細を、コンテンツの配布から不正コピーの発見までの時間的流れに沿って説明する。

【0092】まず、コンテンツの配布に先立ち、購入者装置200の制御部212の制御下で鍵生成部217は、署名鍵と検証鍵を生成する。この生成は、従来の秘密鍵と公開鍵の生成と同じように行う。ここでは、秘密鍵を署名鍵と、公開鍵を検証鍵と呼ぶ。

【0093】次に、鍵生成部217は生成した署名鍵を記憶部220に記憶すると共に、生成した検証鍵を制御部212に渡す。制御部221は、送受信部213を介してプロバイダー装置100に検証鍵を送る。プロバイダー装置100において、送受信部116で受け取られた検証鍵は、記憶部120に記憶される。

【0094】以上の処理が終了した以降において、プロバイダー装置100からコンテンツを購入者装置200に送る場合の動作は次のようになる。

【0095】すなわち、制御部112は、入出力部111と協調して配布するコンテンツを受け入れ、一旦、記憶部120に記憶した後、図4に示すように、暗号化部115を制御し、記憶したコンテンツ121を記憶部120に記憶した検証鍵122を用いて暗号化し（ステップ401）、暗号化したコンテンツを、購入者装置200に送受信部116を介して送信する（ステップ402）。

【0096】一方、暗号化されたコンテンツを受け取った購入者装置100では、次のような処理を行う。

【0097】すなわち、図5に示すように、制御部212は、送受信部213で受け取った暗号化されたコンテンツを復号化部214に、記憶部22に記憶した署名鍵を用いて復号化させ（ステップ501）、次に、署名生成部215に、復号化したコンテンツの記憶部220に記憶した署名鍵を用いた電子署名を生成させる（ステップ502）。

【0098】電子署名の生成は、所定の一方方向ハッシュ関数を用いて、復号化したコンテンツの160ビットのハッシュ値を算出し、この160ビットのハッシュ値を、記憶部220に記憶した署名鍵で暗号化することにより行う。

【0099】電子署名が生成されたならば、制御部212は、署名埋込部を制御し、この電子署名を、所定の規則に従って、復号化したコンテンツに不可分となるよう埋め込み（ステップ503）、記憶部220に記憶する。埋め込みは、たとえば、従来の技術で説明した電子透かしの技術を用いて行う。

【0100】いま、この後、購入者は、記憶部220に記憶された電子署名を埋め込んだコンテンツを不正（コピーする権原を持たずに）にコピーし、第3者に頒布などしてしまった場合を考える。ここで、従来の技術の欄で説明したように、購入者は、電子透かしなどとしてコンテンツにコンテンツと不可分に埋め込んだ電子署名のみをコンテンツから除去して、電子署名なしの完全なコンテンツの不正コピーを作成することはできない。

【0101】この不正コピーされた電子署名が埋め込まれたコンテンツが、押収などされた場合、プロバイダー装置100は、次のようにして、この不正コピーを行った購入者を特定する。

【0102】すなわち、図6に示すように、まず、プロバイダー装置100の制御部112は、入出力部111と協調して不正コピーされたコンテンツを一旦、記憶部120に記憶し、署名抽出部113を制御して、不正コピーされたコンテンツから電子署名を抽出する（ステップ601）。ここで、プロバイダー装置200の記憶部120には、不正コピーされたコンテンツのオリジナルのコンテンツ（電子署名の埋め込まれていないもの）が記憶されているので、このオリジナルのコンテンツと不正コピーされたコンテンツの差分より電子署名を抽出することができる。もしくは、可能な場合には、電子署名をコンテンツに埋め込んだ規則に従って、電子署名をコンテンツから抽出するようにしてもよい。

【0103】次に、制御部112は、署名検証部114を制御し、抽出した電子署名を、記憶部120に記憶した、任意の購入者の検証鍵122で復号化し、復号化した値と、購入者装置200が用いるものと同じ方向ハッシュ関数で記憶部120に記憶しているオリジナルのコンテンツを評価したハッシュ値とを比較することにより、電子署名を検証する（ステップ602）。ここで、購入者装置200が電子署名をコンテンツに埋め込んだ規則がプロバイダー以外に対して秘密化されており、かつ、この規則に基づいて電子署名を、当該電子署名を埋め込んだコンテンツから除去できる場合には、オリジナルのコンテンツに代えて、電子署名を除去したコンテンツを用いるようにしてもよい。

【0104】ここで、オリジナルのコンテンツを評価したハッシュ値と復元した電子署名の値が一致すれば、この不正コピーは、電子署名の復号化に用いた検証鍵に対応する購入者に起因するものであると判断することができる。一致しない場合には、さらに他の購入者の検証鍵を用いて不正コピーから抽出した電子署名を復号化し、オリジナルのコンテンツのハッシュ値との一致を検証する。

【0105】以上、本発明の第1の実施形態について説明した。

【0106】ところで、以上の実施形態において、購入者装置200において、プロバイダー装置100より受け取ったコンテンツの復号化のみを行い、電子署名の埋め込みを行わないと、購入者は自身に関する何の情報も埋め込まないコンテンツを手にすることができ、このようなコンテンツの不正コピーからは購入者を特定することができなくなる。

【0107】そこで、上述した処理部212におけるコンテンツの復号化の処理と電子署名の作成および埋め込みの処理は、一体に行われるように構成する。そして、

これらの処理を分離して行うことのできないようにハードウェア的もしくはソフトウェア的にプロテクトする。具体的には、電子署名の作成および埋め込みの処理が一体に行われるように構成したプログラムをプロバイダーから購入者に提供する。そして、これ以外のプログラムでは、プロバイダー装置 100 から送付されたコンテンツを復号化できないようにする。また、プログラムには適当な改変保護プロテクトを設ける。

【0108】また、たとえば、前述した復号化の処理と電子署名の作成および埋め込みの処理は、図 3 に示した電子計算機の CPU 301 で行うのではなく、プロバイダーが購入者に提供する改変に対するプロテクトを設けた IC カード内で行うようにする。この場合、IC カードを電子計算機に接続して用い、IC カードは、電子計算機から送られた暗号化されたコンテンツに対して、電子署名を埋め込んだコンテンツを返すようにする。

【0109】また、もちろん、改変に対する保護を施した専用のハードウェア装置によって行うようにしてもよい。

【0110】このように第 1 の実施形態によれば、不正コピーに埋め込まれた、購入者自身しか知らないことが保証される署名鍵（秘密鍵）に依存し、購入者自身しか作成することのできない情報を用いて検証することにより、不正コピーの起因となった購入者を判断するので、不正コピーに埋め込まれた情報と、不正コピーの起因となった購入者との対応の証拠性を向上することができる。また、埋め込む情報として、コンテンツの内容に依存するハッシュ値による電子署名を用いるので、不正コピーに埋め込まれた電子署名が示す購入者とコンテンツとの対応性の証拠性も向上することができる。

【0111】ただし、埋め込まれた情報がコンテンツと不可分であることを前提とすれば、コンテンツの内容に依存するハッシュ値による電子署名ではなく、たとえば、プロバイダー装置 100 と購入者装置 200 に対して公開されたデータ、たとえば、購入者名などのテキストのハッシュ値による電子署名を用いても、ある程度、以上の効果を達成することができる。

【0112】以下、本発明の第 2 の実施形態について説明する。

【0113】本第 2 実施形態および後述する第 3 実施形態では、電子データと個人／機関との関係を認証可能とする例として、電子データであるコンテンツの複数の権利者の表示を目的として、コンテンツとコンテンツの複数の権利者との関係を認証可能とする場合を例にとり説明する。ただし、電子データと個人／機関との関係を認証可能とする目的に応じて、本第 2 実施形態および後述する第 3 実施形態は、電子データとの関係を認証可能とする個人／機関を、複数のコンテンツの権利者ではなく、コンテンツの複数の購入者、コンテンツの複数の販売者、コンテンツを取り扱う複数の中間業者、もしくは、

権利者と購入者の組み合わせなどの異なる種類の個人／機関の組み合わせとするように修正してよい。

【0114】さて、本第 2 実施形態は、複数の著作権者などの、配布するコンテンツの複数の権利者の電子署名をコンテンツに埋め込んだ配布コンテンツを作成する配布コンテンツ作成システムについてのものである。

【0115】図 7 に、配布コンテンツ作成システムの構成を示す。

【0116】図示するように、配布コンテンツ作成システムは、1 または複数のコンテンツを配布するプロバイダー装置 100 と、コンテンツの著作権者などの権利者が使用する複数の権利者装置 700 より構成される。プロバイダー装置 100 と権利者装置 700 の間のコンテンツや、その他の情報のやりとりは、プロバイダー装置 100 と権利者装置 700 を結ぶネットワーク 10 を介して行われる。ただし、ネットワーク 10 は必ずしも必要ではなく、プロバイダー装置 100 と権利者装置 700 の間のコンテンツや、その他の情報のやりとりは、当該情報を記憶したフロッピーディスクなどの記憶媒体の運送、郵送などによってもよい。また、この配布コンテンツ作成システムのプロバイダー装置 100、図 1 に示したコンテンツ配布システムのプロバイダー装置 100 を同じプロバイダー装置とすることにより、両システムを一体化するようにしてもよい。図 8 に、この場合のプロバイダー装置 100 と、権利者装置 700 の構成を示す。

【0117】図示するように、プロバイダー装置 100 は、先に図 2 に示したプロバイダー装置と同じ構成を備えており、権利者装置 700 は図 2 に示した購入者装置 200 と同じ構成を備えている。また、第 1 実施形態と同様に、プロバイダー装置 100 も、権利者装置 700 も、図 3 に示したような電子計算機を用いて実現できる。

【0118】さて、このような配布コンテンツシステムにおいて、配布するコンテンツの複数の権利者の電子署名をコンテンツに埋め込んだ配布コンテンツを作成する処理は次の手順によって行われる。

【0119】ただし、プロバイダー装置 100 自身の署名鍵と検証鍵が既に生成されており、プロバイダー装置 100 の検証鍵が各権利者装置に配布されているものとする。また、各権利者装置 700 は、プロバイダー装置 100 へのコンテンツや各種情報を、プロバイダー装置 100 の検証鍵で暗号化して送付し、プロバイダー装置 100 は送付された情報をプロバイダー装置 100 署名鍵で復号化して利用するものとする。なお、この各権利者装置 700 からプロバイダー装置 100 へ送付する情報についての暗号化、復号化に関わる構成は、プロバイダー装置 700 から権利者装置 700 や前述した購入者装置 200 へ送付する情報についての暗号化、復号化に関わる構成と同じであるので、図 7 では図示を省略して

いる。

【0120】さて、このような状況のもと、まず、配布コンテンツの作成に先立ち、権利者装置700は、制御部712の制御下で鍵生成部717は、署名鍵と検証鍵を生成する。この生成は、従来の秘密鍵と公開鍵の生成と同じように行う。

【0121】次に、鍵生成部717は生成した署名鍵を記憶部720に記憶すると共に、生成した検証鍵を制御部712に渡す。制御部721は、送受信部713を介してプロバイダー装置100に検証鍵を送る。プロバイダー装置100において、送受信部116で受け取られた検証鍵は、記憶部120に記憶される。

【0122】以上の処理が終了した以降において、プロバイダー装置100は、複数の権利者の全てについて、順次、権利者の権利者装置700にコンテンツを送付し、当該権利者装置から返却されたコンテンツを次の権利者の権利者装置700に送付する処理を行う。

【0123】すなわち、制御部712は、入出力部711と協調して配布するコンテンツを受け入れ、一旦、記憶部720に記憶した後、暗号化部715を制御し、記憶したコンテンツ721を記憶部720に記憶した、コンテンツを送付しようとする権利者装置700から送られた検証鍵722を用いて暗号化し、暗号化したコンテンツを、権利者装置700に送受信部715を介して送信する。そして、権利者装置700から、当該プロバイダー装置100自身の検証鍵で暗号化されたコンテンツが返却されたならば、これを、当該プロバイダー装置100の署名鍵で復号化し、次にコンテンツを送付する権利者装置700の検証鍵で暗号化し、当該次の権利者装置700に送付する。また、コンテンツの送付の際に、第1番目にコンテンツを送付した権利者装置以外の権利者装置700には、短縮電子署名の使用の指示を添付する。

【0124】一方、プロバイダー装置100から暗号化されたコンテンツを受け取った権利者装置700では、次のような処理を行う。

【0125】すなわち、制御部712は、送受信部713で受け取った暗号化されたコンテンツを復号化部714に、記憶部720に記憶した署名鍵を用いて復号化させ、次に、署名生成部715に、復号化したコンテンツの記憶部720に記憶した署名鍵を用いた電子署名を生成させる。

【0126】電子署名の生成は、所定の一方方向ハッシュ関数を用いて、復号化したコンテンツの160ビットのハッシュ値を算出し、この160ビットのハッシュ値を、記憶部720に記憶した署名鍵で暗号化することにより行う。ただし、送付されたコンテンツに短縮電子署名の使用の指示が添付されている場合には、80ビットのハッシュ値を算出し、この80ビットのハッシュ値を、記憶部720に記憶した署名鍵で暗号化することに

より電子署名を作成する。

【0127】次に、電子署名が生成されたならば、制御部712は、署名埋込部を制御し、この電子署名を、所定の規則に従って、復号化したコンテンツに不可分となるよう埋め込む。埋め込みは、たとえば、従来の技術で説明した電子透かしの技術を用いて行う。そして、電子署名を埋め込んだコンテンツを、送受信部713を介して、プロバイダー装置100に送付することにより返却する。

【0128】この結果、最終的に、プロバイダー装置100に、最後の権利者装置700から返却されたコンテンツには、次のように順次、各権利者の電子署名が埋め込まれることになる。

【0129】すなわち、コンテンツDに対して第i番目の権利者の電子署名が埋め込まれたコンテンツをFi(D)で表すこととすると、まず、第1の権利者はオリジナルのコンテンツの160ビットのハッシュ値である電子署名をコンテンツに埋め込みF1(D)とする。次に、第2の権利者は第1の権利者の電子署名が埋め込まれたコンテンツの80ビットのハッシュ値である電子署名をコンテンツに埋め込み、F2(F1(D))とする。以下同様に、第n番目の権利者は、第1から第1-n番目の権利者の電子署名が埋め込まれたコンテンツの80ビットのハッシュ値である電子署名をコンテンツに埋め込み、Fn(Fn-1(Fn-2(...(F2(F1(D))...))とする。

【0130】プロバイダー装置100は、最終的に最後の権利者から返却された、以上のように順次各権利者の電子署名が埋め込まれたコンテンツを配布コンテンツとする。

【0131】このように、本第2実施形態では、第2番目の権利者以降の権利者の電子署名に用いるハッシュ値のビット数を、第1番目の権利者が電子署名に用いるハッシュ値のビット数の半分としている。これは、既に、電子署名が施されたコンテンツの偽造は、電子署名が施されていないコンテンツを偽造する場合に比べ困難となることから、第2番目以降の権利者の電子署名に用いるハッシュ値のビット数を、第1番目の権利者が電子署名に用いるハッシュ値のビット数の半分としても、そのセキュリティは、各権利者が160ビットの電子署名をオリジナルのコンテンツに施す場合と同様に守られることによるものである。

【0132】電子署名を埋め込んだコンテンツよりの各権利者の検証は、第1実施形態における購入者の検証と同様に行う。

【0133】以下、本発明の第3実施形態を説明する。

【0134】本第3実施形態は、第2実施形態における各権利者の電子署名の埋め込の方法を修正したものである。

【0135】すなわち、第3実施形態では、第1の権利

者は、第2実施形態と同様、プロバイダー装置100から送られたコンテンツのハッシュ値を暗号化して電子署名を生成する。しかし、第1の権利者の権利者装置700は、電子署名をコンテンツに埋め込まずに、電子署名をプロバイダー装置100に返却する。プロバイダー装置100は、返却された第1の権利者の電子署名を、第2の権利者の権利者装置700に送付する。第2の権利者装置700は、送付された第1の権利者の電子署名のハッシュ値を暗号化して自身の電子署名とする。以下、同様に、第2番目以降の権利者の権利者装置700は、前の権利者の電子署名のハッシュ値を暗号化して自身の電子署名とする。

【0136】そして、最後の権利者の権利者装置700の電子署名を受け取ったプロバイダー装置700は、これを、オリジナルのコンテンツに電子透かしなどとして埋め込み配布コンテンツとする。

【0137】ただし、最後の権利者の権利者装置700にプロバイダー装置100からオリジナルのコンテンツを送り、最後の権利者の権利者装置700で最終的な電子署名をコンテンツに埋め込み、これをプロバイダー装置に返却するようにしてもよい。

【0138】また、次のように、電子署名の埋め込みを行うようにしてもよい。すなわち、第1番目の権利者の権利者装置700において、コンテンツのハッシュ値を暗号化した電子署名をコンテンツに埋め込んでプロバイダー装置100を介して第2番目の権利者の権利者装置700に送付するようにし、第2番目以降の権利者の権利者装置700は、受け取った電子署名が埋め込まれたコンテンツから前の権利者の電子署名を抽出し、抽出した電子署名のハッシュ値を暗号化した電子署名を自身の電子署名として作成し、これを、プロバイダー装置100から別途受け取ったオリジナルのコンテンツに埋め込む。もしくは、自身の電子署名に、前の権利者の電子署名が埋め込まれたコンテンツ中の電子署名を入れ替える。そして、自身の電子署名を埋め込んだコンテンツを、プロバイダー装置100を介して次の権利者の権利者装置700に送付する。

【0139】電子署名を埋め込んだコンテンツよりの各権利者の検証は、従来の技術の欄で説明したApplied Cryptography, Jhon Wilsy & Sons, Inc. (1996), pp 39-41における場合と同様である。但し、最後に署名した権利者の電子署名は、電子署名が埋め込まれたコンテンツから抽出する。

【0140】以上、本発明の第3実施形態について説明した。

【0141】第2、第3の実施形態によれば、第2番目以降の権利者の電子署名に用いるハッシュ値を第1番目のものの半分としたり、第2番目以降の権利者の電子署名の対象を前の権利者の電子署名とすることに、より少ない情報量の情報の埋め込みによって、複数の権利者の

電子署名を埋め込むことができるので、コンテンツの情報の質の劣化を少なくすることができる。ただし、埋め込まれた情報がコンテンツと不可分であることを前提とすれば、コンテンツの内容に依存するハッシュ値による電子署名ではなく、たとえば、プロバイダー装置100と権利者装置700に対して公開されたデータ、たとえば、権利者名などのテキストのハッシュ値による電子署名を用いてもよい。

【0142】以下、電子データと個人／機関との関係を認証可能とすると共に、電子データとの関係が認証可能な個人／機関と一致することが保証されるように、当該個人／機関を電子データによって利用者に直接提示する実施形態を、第4から第8実施形態として説明する。

【0143】なお本第4実施形態から第8実施形態においては、電子データとしてwebページを例にとり、webページとの関係を認証可能とする個人／機関がクレジット会社であり、そのクレジット会社のマークを販売者が自webページ植えて使用する場合を例にとり説明する。ただし、これらは一例であり、以下に説明する第4実施形態から第8実施形態は、電子データと個人／機関との関係を認証可能とする目的に応じて、webページとの関係を認証可能とする個人／機関を、webページの発信者や、webページとの関係を承認する何らかの個人／機関（たとえば、webページの評価、推奨機関）など、クレジット会社以外のものに置き換えてもよい。また、同様に、販売者は、webページとの関係を認証可能とする個人／機関のマークを使用するwebページ提供者に置き換えてよい。

【0144】また、本第4実施形態から第8実施形態においては、電子データによる利用者への直接提示を、電子データとの関係を認証可能な個人／機関のロゴマーク（イメージデータ）を用いて行う場合を例にとるが、これは、電子データによる利用者への直接提示を、電子データ利用時に利用者が知覚可能な他の種類のデータ、たとえば、テキストデータやドローイングデータやオーディオデータやビデオデータを用いて行うように修正してもよい。または、電子データと認証可能な関係を持つ者を直接表すものではなく、その者の電子データに対する特定の個人／機関の評価結果などを表すマークを用いるように修正してもよい。

【0145】まず、第4の実施形態について説明する。

【0146】図9に、本第4実施形態に係る認証システムの構成を示す。

【0147】図示するように、認証システムは、商品を買う消費者1100-1～1100-n（以下、単に消費者1100とも称する）と、商品を販売する販売者1110と、各種マークを管理するマーク管理者1120とが利用するシステムであって、図9に示すように、消費者端末1101-1～1101-n（以下、単に消費者端末1101とも称する）と、販売者端末1112と、W

WWWサーバ1113と、マーク管理サーバ1122とが、インターネットのような通信網1140を介して、互いに接続されて構成されている。ここで、マーク管理者1120は、本システムを利用する全てのマーク所有者（販売者1110など）にとって信頼できる公正な機関である。ただし、マーク所有者が自己のマークを管理するマーク管理者120を兼ねるようにしてもよく、この場合、販売者端末1112と、WWWサーバ1113と、マーク管理サーバ1122とは、同一のマシンを用いて構成するようにしてもよい。

【0148】消費者端末1101は、消費者1100が使用する端末である。消費者端末1101は、消費者1100に文書データや画像データなどを表示する表示装置1102と、消費者1100がデータや命令などを入力するための入力装置1103-1や1103-2（以下、単に入力装置1103とも称する）を備えている。消費者1100は、消費者端末1101および通信網1140を介して、販売者1110やマーク管理者1120とデータのやり取りを行う。

【0149】販売者端末1112は、販売者1110が使用する端末である。販売者1110は、販売者端末1112を使って、自己が管理する販売店1111のWebページを作成したり、マーク管理者1120とデータのやり取りを行ったりする。

【0150】WWWサーバ1113は、後述のWWWサーバプログラム1407bが動作するサーバであり、消費者端末1101から同じく後述のブラウザプログラム1204bによるアクセスがあった場合に、WebページDB1114に格納された当該Webページを送信する。該送信されたWebページは消費者端末1101の表示装置1102に表示される。

【0151】マーク管理サーバ1122は、販売者1110からの要求に応じてマークを送付する。さらに、消費者1100からの要求に応じて、該マークの真正性、すなわち、当該要求を受け付ける以前に、自マーク管理サーバ122から販売店1110に送付されたものであるかどうかを確認し、その結果を消費者1100に返送する。

【0152】次に、本第4実施形態の認証システムを構成する消費者端末1101、販売者端末1112、WWWサーバ1113、およびマーク管理サーバ1122について説明する。

【0153】図10は、消費者端末1101のハードウェア構成を示す図である。

【0154】本第1実施形態の消費者端末1101のハードウェア構成は、図9に示すように、表示装置1102と、入力装置1103と、通信網インタフェース1201と、記憶装置1202と、中央処理装置（CPU）1203と、一時記憶装置（メモリ）1204とが、バス1200によって互いに接続されて構成されている。

【0155】表示装置1102は、消費者端末1101を使用する消費者1100にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0156】入力装置1103は、消費者端末1101を使用する消費者1100がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0157】通信網インタフェース1201は、通信網1140を介してWWWサーバ1113や、マーク管理サーバ1122とデータのやり取りを行うためのインタフェースである。

【0158】記憶装置1202は、消費者端末1101で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0159】CPU1203は、消費者端末1101を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0160】メモリ1204には、オペレーティングシステム1204a（以下、単にOS1204aとも称する）や、ブラウザプログラム1204b、あるいは真正性確認プログラムA1204cといった、CPU1203が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0161】ここで、OS1204aは、消費者端末1101全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0162】ブラウザプログラム1204bは、消費者端末1101がWWWサーバ1113と通信し、WebページDB1114に格納されたWebページをダウンロードするためのプログラムである。

【0163】真正性確認プログラムA1204cは、消費者端末1101がマーク管理プログラムA1122と通信し、WWWサーバ1113からダウンロードしたWebページに貼り付けられたマークの真正性を確認するためのプログラムである。

【0164】図11は、販売者端末1112のハードウェア構成を示す図である。

【0165】本第4実施形態の販売者端末1112のハードウェア構成は、図11に示すように、表示装置1301と、入力装置1302と、通信網インタフェース1303と、記憶装置1304と、中央処理装置（CPU）1305と、一時記憶装置（メモリ）1306とが、バス1300によって互いに接続されて構成されている。

【0166】表示装置1301は、販売者端末1112を使用する販売者1110にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレ

イなどで構成される。

【0167】入力装置1302は、販売者端末1112を使用する販売者1110がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0168】通信網インターフェース1303は、通信網1140を介してWWWサーバ1113や、マーク管理サーバ1122とデータのやり取りを行うためのインタフェースである。

【0169】記憶装置1304は、販売者端末1112で使用するプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0170】CPU1305は、販売者端末1112を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0171】メモリ1306には、OS1306aや、Webページ作成プログラム1306b、あるいはマーク取得プログラム1306cといった、CPU1305が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0172】ここで、OS1306aは、販売者端末1112全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0173】Webページ作成プログラム1306bは、販売者1100がWebページを作成する処理と、WWWサーバ1113と通信し、作成したWebページをWebページDB1114に格納する処理とを行うためのプログラムである。

【0174】マーク取得プログラム1306cは、販売者端末1112がマーク管理プログラムA1122と通信し、Webページに貼り付けるマークを取得するためのプログラムである。

【0175】図12は、WWWサーバ1113のハードウェア構成を示す図である。

【0176】本第4実施形態のWWWサーバ1113のハードウェア構成は、図12に示すように、表示装置1401と、入力装置1402と、通信網インターフェース1403と、WebページDBインターフェース1404と、記憶装置1405と、中央処理装置(CPU)1406と、一時記憶装置(メモリ)1407とが、バス1400によって互いに接続されて構成されている。

【0177】表示装置1401は、WWWサーバ1113を使用する販売者1110にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0178】入力装置1402は、WWWサーバ1113を使用する販売者1110がデータや命令などを入力するために用いられるものであり、キーボードやマウス

などで構成される。

【0179】通信網インターフェース1403は、通信網1140を介して消費者端末1101や、販売者端末1112とデータのやり取りを行うためのインタフェースである。

【0180】WebページDBインターフェース1404は、WebページDB1114とデータのやり取りを行うためのインタフェースである。

【0181】記憶装置1405は、WWWサーバ1113で使用するプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0182】CPU1406は、WWWサーバ1113を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0183】メモリ1407には、OS1407aやWWWサーバプログラム1407bといった、CPU1406が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0184】ここで、OS1407aは、WWWサーバ1113全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0185】WWWサーバプログラム1407bは、販売者端末1112と通信し、受け取ったWebページをWebページDB1114に格納する処理と、消費者端末1101からブラウザプログラム1204bによるアクセスがあった場合に、WebページDB1114に格納されている当該Webページを送信する処理とを行うためのプログラムである。

【0186】図13は、マーク管理サーバ1122のハードウェア構成を示す図である。

【0187】本第4実施形態のマーク管理サーバ1122のハードウェア構成は、図13に示すように、表示装置1501と、入力装置1502と、通信網インターフェース1503と、マーク管理DBインターフェース1504と、記憶装置1505と、中央処理装置(CPU)1506と、一時記憶装置(メモリ)1507とが、バス1500によって互いに接続されて構成されている。

【0188】表示装置1501は、マーク管理サーバ1122を使用するマーク管理者1120にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0189】入力装置1502は、マーク管理サーバ1122を使用するマーク管理者1120がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0190】通信網インターフェース1503は、通信網1140を介して消費者端末1101や、販売者端末1112とデータのやり取りを行うためのインタフェー

スである。

【0191】マーク管理DBインターフェース1504は、マーク管理DB1123とデータのやり取りを行うためのインターフェースである。該マーク管理DB1123は、マークの種別や、当該マークの有効期限、販売者の識別情報、あるいは販売店のWebページのURLなどといったデータを対応づけて管理するものであり、たとえば図15のようなものである。図15において、マークに有効期限を設けない場合、また、マーク管理者120がただ一つのマークのみを発行する場合には、それぞれに対応する項目、すなわち有効期限やマーク種別などを管理しなくてよいのは明らかである。

【0192】記憶装置1505は、マーク管理サーバ1122で使用するプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0193】CPU1506は、マーク管理サーバ1122を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0194】メモリ1507には、OS1507aやマーク管理プログラムA1507bといった、CPU1506が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0195】ここで、OS1507aは、マーク管理サーバ1122全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0196】マーク管理サーバプログラムA1507bは、販売者端末1112からマーク送付要求があった場合に、販売者1110を確認してマークを送付するか否かを判定した後、送付すべきであると判定した場合にのみ、マーク管理DB1123によって管理されているマークを販売者1110に送信する処理と、消費者端末1101からマークの真正性確認要求があった場合に、マーク管理DB1123を参照して当該マークの真正性を検証し、その結果を返送する処理とを行うためのプログラムである。

【0197】次に、本第4実施形態の認証システムの動作について説明する。

【0198】図14は、販売者1110がマーク管理者1120からマークを受け取り、該マークを自己のWebページに貼り付けてから公開した後、消費者1100が当該Webページを閲覧して、該Webページの真正性を確認する場合の、消費者1100と販売者1110、およびマーク管理者120の動作を説明するための図である。

【0199】図14において、消費者1100が行う処理には消費者端末1101が使用され、販売者1110が行う処理には販売店端末1112およびWWWサーバ1113が使用される。また、マーク管理者1120が

行う処理にはマーク管理サーバ1122が使用される。

【0200】まず、販売者1110は、自己のWebページのURLやマーク種別などを含むマーク送付要求をマーク管理者1120に送る（ステップ1600）。

【0201】要求を受けたマーク管理者1120は、当該要求に含まれるマーク種別で指定されたマークを販売者1110に対して送付するか否かを判定し（ステップ1601）、送付すると判定した場合にのみ、マーク管理DB1123を更新した後（ステップ1602）、当該マークを販売者1110に送付する（ステップ1603）。また、送付しないと判定した場合にはその旨を販売者1110に通知する。本第4実施形態での送付するか否かの判定は、販売者1110が当該マークを取得する権利を有しているか否か、すなわち当該マークをロゴとして使用しているクレジットカード会社の加盟店であるか否か、ということに基づいて行う。しかし、これは、マークを交付する目的に応じて別の基準を用いてもよい。

【0202】マークを受け取った販売者1110は、該マークを自己のWebページに貼り付けてマーク付きWebページを作成するとともに（ステップ1604）、該マークにマーク管理者1120へのリンク情報を設定し（ステップ1605）、当該Webページを消費者1100からアクセス可能な状態でWebページDB1114に格納する（ステップ1606）。

【0203】次に、消費者1100は、上記WebページのURLを含んだWebページ送付要求を販売者1110に送る（ステップ1607）。

【0204】要求を受け取った販売者1110は、WebページDB1114を検索し（ステップ1608）、当該URLに対応したWebページを消費者1100に返送する（ステップ1609）。

【0205】Webページを受け取った消費者1100は、さらに、表示された（ステップ1610）該Webページに貼り付けられたマークをクリックし（ステップ1611）、当該WebページのURLなどを含む真正性確認要求をマーク管理者1120に送る（ステップ1611）。その際、もし、上記マークにマーク管理者1120へのリンク情報が正しく設定されていないためにマーク管理者1120への真正性確認要求を送れなかった場合には、消費者1100は、該マークの真正性が確認されなかったもの（にせのマーク）と判断して、全ての処理を終了する。

【0206】要求を受け取ったマーク管理者1120は、マーク管理DB1123を検索して、当該要求に含まれるURLで指定された販売者1110に対して、すでにマークを送付しているか否か、また、送付している場合、該マークが有効期限内であるかどうかを確認する（ステップ1612）。そして、<1>:URLで指定された販売店1110にはマークを発行していない、<2>:U

R Lで指定された販売店 1110 にマークを発行しているが、すでに有効期限がきれている、<3>URLで指定された販売店 1110 にマークを発行しており、かつ、そのマークは有効期限内である、といった3種類の結果のいずれか一つを、消費者 1100 に送付する(ステップ 613)。

【0207】最後に、上記結果を消費者 1100 が確認して全ての処理が終了する(ステップ 614)。

【0208】上記手順において、消費者 1100 による真正性の確認は、たとえば、図 9 に示すように表示装置 1102 に「本物です」(あるいは「にせものです」、「期限切れです」、「リンク情報が正しく設定されていません」)といった吹き出しが表示され、消費者 1100 が該吹き出しを見ることによって行われる。しかし、これは、別の表示方法を用いてもよい。また、音などを用いて行ってもよいし、音、表示を組み合わせてもよい。

【0209】さて、本第 4 実施形態では、マーク管理者 1120 はマークを受け取る権利がある販売店 1110 にのみマークを送付するようにしている。そして、マークの関連情報(送付した販売店 1110 の識別情報や Web ページの URL、マークの有効期限など)をマーク管理 DB 1123 で管理するようにしている。さらに、該マーク管理 DB 1123 を参照し、消費者 1100 から送られてきた真正性確認要求に含まれる URL が示す販売店 1110 に対して、すでにマークを送付しているか否か、また、送付している場合には、そのマークが有効期限内のものであるか否かを確認して、消費者に通知するようにしている。

【0210】また、消費者 1100 は、Web ページに貼り付けられたマークに設定されたリンク情報を使って、マークの真正性をマーク管理者 1120 に確認するようにしている。さらに、マーク管理者 1120 へのリンク情報が正しく設定されていないためにマーク管理者 1120 への真正性確認要求を送れなかった場合には、該マークの真正性が確認されなかったもの(にせのマーク)と判断するようにしている。

【0211】したがって、本第 4 実施形態によれば、不正者が自己の Web ページに、正規販売者の Web ページからコピーしたマークを貼り付けた場合は、マーク管理者が管理するマーク管理 DB に不正者の Web ページにマークを送付した記録がないため、真正性確認処理で該マークの真正性が確認されない。結果として販売者の Web ページを閲覧する消費者が、その Web ページに貼り付けられたマークが明示する情報が真正なものであるか否かを正しく確認することができることになる。

【0212】なお、本第 4 実施形態では、消費者 1100 がマークをクリックすることで真正性確認処理が開始されるようにしているが、これは、Web ページを受け取ったときに自動的に真正性確認処理が開始されるよう

にしてもよい。さらに、該処理において真正性が確認された場合に、当該 Web ページが表示されるようにしてもよい。

【0213】また、本第 4 実施形態では、販売者端末 112 と WWW サーバ 113 とを別マシンとして説明したが、これは同一のマシンであってもよい。

【0214】以下、本発明の第 5 実施形態について説明する。

【0215】図 16 に、本第 5 実施形態に係る認証システムの構成を示す。

【0216】本第 5 実施形態の認証システムの構成は、基本的には図 9 に示したものと同じである。ただし、各消費者端末 1800-1~1800-n (以下、単に消費者端末 1800 と称する)に、それぞれ公開鍵 DB 1801-1~1801-n (以下、単に公開鍵 DB 1801 と称する)が接続されている点異なる。

【0217】公開鍵 DB 1810 は、マーク管理者の公開鍵を管理するものであり、たとえば図 20 のようなものである。これらの公開鍵は、当該マーク管理者が生成したデジタル署名(以下、単に署名とも称する)を検証する際に用いられる。

【0218】図 17 は、本第 5 実施形態の消費者端末 1800 のハードウェア構成を示す図である。

【0219】本第 5 実施形態の消費者端末 800 のハードウェア構成は、基本的には図 10 に示したものと同じである。ただし、公開鍵 DB インタフェース 1900 を備えている点と、メモリ 1901 上に真正性確認プログラム B902 が格納され、実行される点とが異なる。

【0220】公開鍵 DB インタフェース 1900 は、公開鍵 DB 1801 とデータのやり取りを行うためのインターフェースである。また、真正性確認プログラム B1902 は、マーク管理サーバ 1810 と通信し、マーク管理者 1120 の公開鍵を取得する処理と、該公開鍵を用いて、WWW サーバ 113 からダウンロードした Web ページに貼り付けられた署名付きマークの真正性を確認する処理とを行うためのプログラムである。

【0221】図 18 は、本実施形態のマーク管理サーバ 1810 のハードウェア構成を示す図である。

【0222】本第 5 実施形態のマーク管理サーバ 1810 のハードウェア構成は、基本的には図 13 に示したものと同じである。ただし、メモリ 11000 上にマーク管理プログラム B11001 が格納され、実行される点異なる。

【0223】マーク管理プログラム B11001 は、消費者端末 1800 から公開鍵送付要求があった場合に、自己の公開鍵を送付する処理と、販売者端末 1112 からマーク送付要求があった場合に、販売者 1110 を確認してマークを送付するか否かを判定した後、送付すべきであると判定した場合にのみ、該販売者 1110 の Web ページの URL を示すデータに秘密鍵を用いて電子

署名を作成し、電子署名とマーク管理DB1123によって管理されているマークとを一纏めにして署名付きマークを作成し、該署名付きマークを販売者1110に送信する処理とを行うためのプログラムである。電子署名とマークとを一纏めにするには、たとえば、前述した電子透かし技術を利用し、マークに電子署名による電子透かしを施すことにより可能となる。電子透かしは、画像データに微少な変更を加えることで、情報を埋め込む技術である。マークは画像データの種類であることから、電子透かしを用いて任意の情報を埋め込むことができる。また、電子透かしには、カラー画像用、白黒画像用、2値画像用などがあるので、各種のマークへの情報埋込みが可能である。しかし、これは別の手法を用いてもよい。なお、マークと電子署名とを一纏めにする手段として電子透かしを用いる場合、マークの視認性さえ阻害しなければ（たとえば、どこのクレジットカード会社のロゴマークだということがわかれば）、マーク自体は多少変形されてもよい。

【0224】また、署名に用いる公開鍵暗号方式としては、素因数分解を用いるもの、楕円曲線を用いるものなどが使用可能である。

【0225】次に、本第5実施形態の認証システムの動作について説明する。

【0226】図19は、消費者1100がマーク管理者1120の公開鍵を取得した後、販売者1110がマーク管理者1120からマークを受け取り、該マークを自己のWebページに貼り付けてから公開し、さらに、消費者1100が当該Webページを閲覧して、該Webページの真正性を確認する場合の、消費者1100と販売者1110、およびマーク管理者1210の動作を説明するための図である。

【0227】図19において、消費者1100が行う処理には消費者端末1800が使用され、販売者1110が行う処理には販売店端末1112およびWWWサーバ1113が使用される。また、マーク管理者1120が行う処理にはマーク管理サーバ1810が使用される。

【0228】まず、消費者1100は、公開鍵送付要求をマーク管理者1120に送る（ステップ11100）。

【0229】要求を受け取ったマーク管理者1120は（ステップ11101）、自己の公開鍵を消費者1100に返送する（ステップ11102）。

【0230】マーク管理者1120の公開鍵を受け取った消費者1100は、該公開鍵を公開鍵DB1801に格納する（ステップ11103）。

【0231】次に、販売者1110は、自己のWebページのURLやマーク種別などを含むマーク送付要求をマーク管理者1120に送る（ステップ11104）。

【0232】要求を受けたマーク管理者1120は、当該要求に含まれるマーク種別で指定されたマークを販売

者1110に対して送付するか否かを判定し（ステップ11105）、送付すると判定した場合にのみ、当該要求に含まれるURLデータに秘密鍵を用いて署名を施し、該署名とマーク種別で指定されたマークとを一纏めにして署名付きマークを生成する（ステップ11106）。そして、該署名付きマークを販売者1110に送付する（ステップ11107）。また、送付しないと判定した場合にはその旨を販売者1110に通知する。本実施形態での送付するか否かの判定も、第4の実施形態と同様、販売者1110が当該マークを取得する権利を有しているか否か、すなわち当該マークをロゴとして使用しているクレジットカード会社の加盟店であるか否か、ということに基づいて行う。ただし、他の適当な基準を用いてもよい。

【0233】署名付きマークを受け取った販売者1110は、該署名付きマークを自己のWebページに貼り付けてマーク付きWebページを作成し（ステップ11108）、当該Webページを消費者1100からアクセス可能な状態でWebページDB1114に格納する（ステップ11109）。

【0234】次に、消費者1100は、上記WebページのURLを含んだWebページ送付要求を販売者1110に送る（ステップ11110）。

【0235】要求を受け取った販売者1110は、WebページDB1114を検索し（ステップ11111）、当該URLに対応したWebページを消費者1100に返送する（ステップ11112）。

【0236】Webページを受け取った消費者1100が、表示された（ステップ11113）該Webページに貼り付けられた署名付きマークをクリックすると（ステップ11114）、公開鍵DB1801に格納されたマーク管理者1120の公開鍵と該WebページのURLとを用いて、該署名付きマークに含まれる署名の検証が行われる（ステップ11115）。そして、署名が正しく検証されたか否かにより、消費者1100が当該署名付きマークの真正性を確認して全ての処理が終了する（ステップ11116）。

【0237】上記手順において、消費者1100による真正性の確認は、たとえば、図16に示すように表示装置102に「本物です」（あるいは「にせものです」、「必要な公開鍵がありません」）といった吹き出しが表示され、消費者1100が該吹き出しを見ることによって行われる。しかし、別の表示方法を用いてもよい。また、音などを用いて行ってもよいし、音、表示を組み合わせてもよい。

【0238】上記の本第5実施形態では、マーク管理者120は署名付きマークを受け取る権利がある販売店1110にのみ署名付きマークを送付するようにしている。そして、署名付きマークを生成するときの要素として、販売店1110のWebページのURLデータを用

いている。

【0239】また、消費者1100は、Webページに貼り付けられた署名付きマークの署名を、マーク管理者の公開鍵と該WebページのURLデータとを使って検証するようにしている。

【0240】したがって、本第5実施形態によれば、不正者が自己のWebページに、正規販売者のWebページからコピーした署名付きマークを貼り付けた場合は、不正者のWebページのURLと署名に含まれるURLとが一致しないため、真正性確認処理で該マークの真正性が確認されない。結果として販売者のWebページを閲覧する消費者が、そのWebページに貼り付けられたマークが明示する情報が真正なものであるか否かを正しく確認することができる。

【0241】なお、本第5実施形態では、消費者1100がマークをクリックすることで真正性確認処理が開始されるようにしているが、第4実施形態と同様、Webページを受け取ったときに自動的に真正性確認処理が開始されるようにしてもよい。さらに、該処理において真正性が確認された場合に、当該Webページが表示されるようにしてもよい。

【0242】なお、本実施形態における、販売者110がマークを取得するステップと消費者1100が公開鍵を取得するステップとの前後関係は逆でもよい。ただし、本第5実施形態のように、ステップ11110からはじまるWebページアクセス以前に、消費者11100が公開鍵を取得しておけば、Webページアクセスの度に公開鍵を取得する必要がない。

【0243】また、本第5実施形態では、販売者端末1112とWWWサーバ1113とを別マシンとしているが、同一のマシンであってもよい。

【0244】さらに、また、本第5実施形態では、WebページのURLデータの上に署名を施すようにしているが、たとえば、マークとして用いている画像データを電子署名の対象に加えてもよい。これにより、販売店1110がマーク管理者1120より受け取った署名付きマークの署名部分だけを取り出し、自分が加盟店契約していないクレジットカード会社のマークと一緒にし直すことで、にせの署名付きマークを生成するといった不正を防ぐことができ、より安全性が高まる。さらに、たとえば、販売者1110がマークを貼り付けるWebページをあらかじめ生成し、それをマーク送付要求時にマーク管理者1120に送るようにし、該Webページを電子署名の対象に加えてもよい。これにより、別のWebページに署名付きマークを貼り付けることができなくなり、たとえば、署名付きマークをWebページの内容証明手段として利用することができるようになる。すなわち、この変形例は、何らかの権威者にWebページの内容を保証してもらうようなシステムでの利用に適している。

【0245】くわえて、本第5実施形態では、署名とマークとを一纏めにして署名付きマークを生成しているが、これは、たとえば、販売者110がマークを貼り付けるWebページをあらかじめ生成し、それをマーク送付要求時にマーク管理者120に送るようにし、マーク管理者120が該Webページの内容に基づいて作成したフィルタリング用データなどを属性情報として署名付きマークに加えてもよい。

【0246】これにより、たとえば、あるWebページ評価機関が発行した推奨マークが貼られ、かつ、その真正性が正しく確認されたWebページのみを表示するようフィルタリングすることができる。そのためには、どの種類のマークなら消費者端末1101の表示装置1102に表示するかということを消費者1100に設定させるためのフィルタリング設定機能や、それ以外のものなら表示しないようにするようなフィルタリング実行機能などを備えたフィルタリングプログラムを、あらかじめ消費者端末1101にインストールしておけばよい。この応用例は、たとえば子どもに見せたくないような暴力表現などを含んだWebページをフィルタリングしたようなシステムでの利用に適している。

【0247】なお、第4、第5実施形態の各端末、サーバに格納された各プログラムは、一般的には、それぞれの装置を制御するオペレーティングシステムの下で動作し、オペレーティングシステムを介して、装置の各ハードウェア構成要素とデータ、コマンドをやりとりする。もちろん、オペレーティングシステムを介さずに直接、各ハードウェア構成要素とデータ、コマンドをやりとりしても良い。

【0248】以上説明したように、第4、第5実施形態によれば、Webページを閲覧するユーザが、そのWebページに貼り付けられた画像データが明示する情報（ユーザが見た目から判断するであろう情報）が真正なものであるか否かを正しく確認することができる。

【0249】以下、本発明の第6の実施形態について説明する。

【0250】本第6実施形態の認証システムの構成は、基本的には前記第1実施形態に係る認証システムの構成（図9から図13参照）と同じである。ただし、消費者端末1101のメモリ1204中の真正性確認プログラムA1204cが真正性確認プログラムCに置き換えられ、マーク管理サーバ1122のメモリ1507中のマーク管理プログラムA1507bが、マーク管理プログラムCに置き換えられ、販売者端末112のメモリ1306中のマーク取得プログラムが1306がマーク取得プログラムCに置き換えられた構成となっている。

【0251】以下、本第6実施形態に係る認証システムの動作について説明する。

【0252】まず、販売者端末1112のマーク取得プログラムCは、自己のWebページのデータと共にマー

ク送付要求をマーク管理サーバ1122に送る。

【0253】要求を受けたマーク管理サーバ1122の、マーク管理プログラムCは、要求を送った販売者端末1112を使用する販売者1110に対してマークを送付するか否かを判定し、送付すると判定した場合、図21に示す処理を行う。

【0254】すなわち、マーク管理DB1123に格納しておいたマーク2709と、マークに挿入する所定の情報2708（たとえば、マーク管理機関1121を示すテキストなど）を読み出し、マークに所定の情報を電子透かしとして埋め込む（ステップ2705）。そして、電子透かしを埋め込んだマーク2710がWebページ上に表示されるように、マーク送付要求と共に送られたWebページデータ2711を修正し（ステップ2706）、修正したWebページデータ2712を販売者端末1112のマーク取得プログラムcに送る（ステップ2707）。

【0255】マーク取得プログラムcは、マーク管理サーバ1122から送られたWebページデータを、WWWサーバ1113を介して、webページデータベース1114に格納する。

【0256】その後、このwebページは、消費者端末1101のブラウザプログラム1204bを介した消費者1100の要求に応じて消費者端末1101に送られ、表示装置1102に表示される。

【0257】一方、消費者端末1101の、真正性確認プログラムCは、消費者1100からの要求に応じて（たとえばマークのクリックに応じて）、webページの真正性確認処理を行う。

【0258】この処理では、図22に示すように、まず、webページ2908から真正性を確認するマーク2909を切り出し（ステップ2905）、切り出したマーク2909に電子透かしとして埋め込まれた情報2910を抽出し（ステップ2906）、これを表示装置1102に表示する（ステップ2907）。

【0259】ここで、切り出したマーク2909から電子透かしとして埋め込まれた情報2910を抽出するために必要な情報（この情報としては、たとえば、図21の710の電子透かしが施される前のオリジナルのマークや、オリジナルのマークとの差分より情報を復元するためのアルゴリズムを特定する情報などが該当する場合がある）は、マーク管理サーバ1122から予め入手しておくようにする。このためには、真正性確認プログラムC2204が消費者1100の要求に応じてマーク管理サーバ1122に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ1204や記憶装置1202に記憶しておくようにする。また、マーク管理サーバ1122の、マーク管理プログラムC2507bは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末1101に送るようにする。

【0260】以上、本発明の第6の実施形態について説明した。

【0261】本第6実施形態によれば、単なるマークに代えて、電子透かしを施したマークをwebページ上に設けるので、そのマークよりwebページとマークが示す個人／機関との関係の真正性が認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人／機関を提示することができ、また、webページ上の存在に不自然さのないマークを利用してwebページとマークが示す個人／機関との関係の真正性が認証可能とするので、本第6実施形態によってwebページが不自然な形態に損なわれることはない。

【0262】以下、本発明の第7実施形態について説明する。

【0263】本第7実施形態の認証システムの構成は、基本的には前記第1実施形態に係る認証システムの構成（図9から図13参照）と同じである。ただし、消費者端末1101のメモリ1204中の真正性確認プログラムA1204cが真正性確認プログラムdに置き換えられ、マーク管理サーバ1122のメモリ1507中のマーク管理プログラムA1507bが、マーク管理プログラムdに置き換えられ、販売者端末112のメモリ1306中のマーク取得プログラムが1306がマーク取得プログラムdに置き換えられた構成となっている。

【0264】以下、本第7実施形態に係る認証システムの動作について説明する。

【0265】まず、販売者端末1112のマーク取得プログラムdは、自己のWebページのデータと共にマーク送付要求をマーク管理サーバ1122に送る。

【0266】要求を受けたマーク管理サーバ1122の、マーク管理プログラムdは、要求を送った販売者端末1112を使用する販売者1110に対してマークを送付するか否かを判定し、送付すると判定した場合、図23に示す処理を行う。

【0267】すなわち、マーク送付要求と共に送られたWebページデータ2305のハッシュ値2306を計算し（ステップ2301）、マーク管理DB1123に格納しておいたマーク2307に、計算したハッシュ値2306を電子透かしとして埋め込む（ステップ2302）。そして、電子透かしを埋め込んだマーク2308がWebページ上に表示されるように、マーク送付要求と共に送られたWebページデータ2305を修正し（ステップ2302）、修正したWebページデータ2309を販売者端末1112のマーク取得プログラムdに送る（ステップ2304）。

【0268】マーク取得プログラムdは、マーク管理サーバ1122から送られたWebページデータを、WWWサーバ1113を介して、webページデータベース1114に格納する。

【0269】その後、このwebページは、消費者端末1101のブラウザプログラム1204bを介した消費者1100の要求に応じて消費者端末1101に送られ、表示装置1102に表示される。

【0270】一方、消費者端末1101の、真正性確認プログラムdは、消費者1100からの要求に応じて（たとえばマークのクリックに応じて）、webページの真正性確認処理を行う。

【0271】この処理では、図24に示すように、まず、webページ2406から真正性を確認するマーク2407を切り出し（ステップ2401）、切り出したマーク2407に電子透かしとして埋め込まれたハッシュ値2408を抽出する（ステップ2402）。また、webページ2406から真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値2409を計算し（ステップ2409）、これとマークから抽出したハッシュ値2408とを比較する（ステップ2404）。そして、一致した場合には、真正性が確認できたことを、一致しない場合には、真正性が確認できなかったことを表示装置1102に表示する（ステップ2405）。

【0272】なお、切り出したマークから電子透かしとして埋め込まれたハッシュ値を抽出するために必要な情報は、マーク管理サーバ1122から予め入手しておくようにする。このためには、真正性確認プログラムdが消費者1100の要求に応じてマーク管理サーバ1122に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ1204や記憶装置1202に記憶しておくようにする。また、マーク管理サーバ1122の、マーク管理プログラムdは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末1101に送るようにする。

【0273】本第7実施形態によれば、単なるマークに代えて、webページのハッシュ値を電子透かしとして施したマークをwebページ上に設けるので、そのマークより当該マークが確かに、そのマークを含むwebページに対して与えられたものであることが認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人／機関を提示することができる。また、電子透かしとしてwebページデータのハッシュ値を用い、これを特定の種類のデータであるマークの電子透かしとして用いるので、webページが複数種のデータを含んでいるかどうかにかかわらず、同一の処理で処理を行うことができる。また、webページ上の存在に不自然さのないマークを利用して、webページに対して真にマークが与えられたことを認証可能とするので、本第7実施形態によってwebページが不自然な形態に損なわれることはない。

【0274】以下、本発明の第8の実施形態について説明する。

【0275】本第8実施形態に係る認証システムは、基本的には前記第1実施形態に係る認証システムの構成（図9から図13参照）と同じである。

【0276】ただし、消費者端末1101については、図25に示すように、前記第5実施形態で説明した公開鍵DB1801が接続されている点と、公開鍵DBインタフェース1900を備えている点と、メモリ1204中の真正性確認プログラムA1204cが真正性確認プログラムe3204に置き換えられている点と異なる。

【0277】また、マーク管理サーバ1122については、図26に示すように、メモリ1507中のマーク管理プログラムA1507bが、マーク管理プログラムe3507に置き換えられている点と異なる。

【0278】また、図27に示すように、販売者端末112については、メモリ1306中のマーク取得プログラムが1306がマーク取得プログラムe3306に置き換えられた構成となっている点と異なる。

【0279】以下、本第8実施形態に係る認証システムの動作について説明する。

【0280】まず、販売者端末1112のマーク取得プログラムdは、自己のWebページのデータと共にマーク送付要求をマーク管理サーバ1122に送る。

【0281】要求を受けたマーク管理サーバ1122の、マーク管理プログラムdは、要求を送った販売者端末1112を使用する販売者1110に対してマークを送付するか否かを判定し、送付すると判定した場合、図28に示す処理を行う。

【0282】すなわち、マーク送付要求と共に送られたWebページデータ2806のハッシュ値2807を計算し（ステップ2801）、ハッシュ値2807をマーク管理機関の秘密鍵2808で暗号化した電子署名2809を作成し（ステップ2802）、これをマーク管理DB1123に格納しておいたマーク2810に、電子透かしとして埋め込む（ステップ2803）。そして、電子透かしを埋め込んだマーク2811がWebページ上に表示されるように、マーク送付要求と共に送られたWebページデータ2806を修正し（ステップ2804）、修正したWebページデータ2812を販売者端末1112のマーク取得プログラムeに送る（ステップ2805）。

【0283】マーク取得プログラムeは、マーク管理サーバ1122から送られたWebページデータを、WWWサーバ1113を介して、webページデータベース1114に格納する。

【0284】その後、このwebページは、消費者端末1101のブラウザプログラム1204bを介した消費者1100の要求に応じて消費者端末1101に送られ、表示装置1102に表示される。

【0285】一方、消費者端末1101の、真正性確認プログラムdは、消費者1100からの要求に応じて

(たとえばマークのクリックに応じて)、webページの真正性確認処理を行う。

【0286】この処理では、図29に示すように、まず、公開鍵DB1801からマーク管理機関の公開鍵2908を取り出す。そして、webページ2907から真正性を確認するマーク2908を切り出し(ステップ2901)、切り出したマーク2908に電子透かしとして埋め込まれた電子署名2909を抽出し(ステップ2902)、マーク管理機関の公開鍵2910により復号化してハッシュ値を抽出する(ステップ2903)。また、webページ2907から真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値2912を計算し(ステップ2904)、これとマークから抽出した電子署名を復号化したハッシュ値2911とを比較する(ステップ2905)。そして、一致した場合には、真正性が確認できたことを、一致しない場合には、真正性が確認できなかったことを表示装置1102に表示する(ステップ2906)。

【0287】なお、切り出したマークから電子透かしとして埋め込まれたハッシュ値を抽出するために必要な情報は、マーク管理サーバ1122から予め入手しておくようにする。このためには、真正性確認プログラムeが消費者1100の要求に応じてマーク管理サーバ1122に真正性確認用情報の要求を送り、その応答として送られた情報をメモリ1204や記憶装置1202に記憶しておくようにする。また、マーク管理サーバ1122の、マーク管理プログラムeは、真正性確認用情報の要求を受け取った場合には、必要な情報を消費者端末1101に送るようにする。

【0288】また、マーク管理機関の公開鍵は、消費者端末1100より、公開鍵送付要求をマーク管理サーバ1113に送り、その応答として受けとった公開鍵を公開鍵DB1801に格納するようにする。また、公開鍵送付要求を受け取ったマーク管理サーバ1113は、自己の公開鍵を応答として消費者端末1100に返送するようにする。

【0289】以上のように、本第8実施形態によれば、単なるマークに代えて、webページのハッシュ値をマーク管理機関の秘密鍵で暗号化した電子署名を電子透かしとして施したマークをwebページ上に設けるので、そのマークより当該マークが確かに、そのマークを含むwebページに対して、マーク管理機関によって与えられたものであることが認証可能となるのみならず、webページによって直接、マークの形態で、そのwebページと関係がある個人/機関を提示することができる。また、webページデータのハッシュ値を対象とした電子署名を、これを特定の種類のデータであるマークの電子透かしとして用いるので、webページが複数種のデータを含んでいるかどうかは依存することなく、同一の処理で処理を行うことができる。また、電子署名を電子透かしとしてwe

bページ上のマークに埋め込むので、webページデータと別個に電子署名を管理する必要はない。また、存在に不自然さのないマークを利用して、webページと個人/機関の関係を認証可能とするので、本第8実施形態によってwebページが不自然な形態に損なわれることはない。

【0290】なお、以上の第6実施形態から第8実施形態では、マーク管理サーバ1122において、電子透かしを埋め込んだマークがWebページ上に表示されるように、マーク送付要求と共に送られたWebページデータを修正し(ステップ2804)、修正したWebページデータ2812を販売者端末1112のマーク取得プログラムeに送る処理を行ったが、これは、次のように修正するようにしてもよい。

【0291】すなわち、マーク管理サーバ1122において、電子透かしを埋め込んだマークを販売者端末1112に送る。そして、販売者端末1112において、電子透かしを埋め込んだマークがWebページ上に表示されるように、マーク送付要求と共に送ったWebページデータのオリジナルを修正する。

【0292】また、以上の第6実施形態から第8実施形態では、消費者端末1101における処理に変えて次の処理を行うようにしてもよい。

【0293】すなわち、第6実施形態の場合は、消費者端末1101は、webページから真正性を確認するマークを切り出し、切り出したマークと共にマーク管理サーバ1122に真正性確認を要求する。また、第7、第8実施形態の場合は、マークを含むwebページのデータと共にマーク管理サーバ1122に真正性確認を要求する。そして、この要求の応答として、マーク管理サーバ1122から送られた、真正性が確認できた、もしくは、真正性が確認できなかった旨のメッセージを表示装置1102に表示する。一方、マーク管理サーバ1122は、真正性確認を要求されたならば、その要求と共に送られたマークについて、第6実施形態から第8実施形態で消費者端末1101において行っていた処理を行う。すなわち、第6実施形態の場合は、要求と共に送られたマークに電子透かしとして埋め込まれた情報を抽出し、これがマーク管理サーバ1122において埋め込んだ情報と一致していれば、真正性が確認できた旨のメッセージを消費者端末1101に送り、一致していなければ真正性が確認できなかった旨のメッセージを消費者端末1101に送る。また、第7実施形態の場合は、要求と共に送られたwebページからマークを切り出し、切り出したマークに電子透かしとして埋め込まれたハッシュ値を抽出し、要求と共に送られたwebページから真正性を確認するマークに関連する部分を除いたwebページデータのハッシュ値を計算し、これとマークから抽出したハッシュ値2408とを比較する。そして、一致した場合には、真正性が確認できた旨のメッセージを消費者端末1101に送り、一致していなければ真正性が確認でき

なかった旨のメッセージを消費者端末 1101 に送る。また第 8 実施形態の場合は、要求と共に送られた web ページからマークを切り出し、切り出したマークに電子透かしとして埋め込まれた電子署名を抽出し、マーク管理機関の公開鍵により復号化してハッシュ値を抽出する。また、要求と共に送られた web ページから真正性を確認するマークに関連する部分を除いた web ページデータのハッシュ値を計算し、これとマークから抽出した電子署名を復号化したハッシュ値とを比較する。そして、一致した場合には、真正性が確認できた旨のメッセージを消費者端末 1101 に送り、一致してなければ真正性が確認できなかった旨のメッセージを消費者端末 1101 に送る。

【0294】ところで、以上の第 6 実施形態から第 8 実施形態は、web ページの他、各種電子商取引の対象となる電子データについて適用可能である。たとえば、各種電子商取引の対象が、図面を表すドローデータである場合に、当該図面に販売者のマークを付けて、当該図面が真正なものであることを認証可能とするような用途に使用することができる。また、前述したように、マークは必ずしもイメージデータでなくてもよい。たとえば、各種電子商取引の対象がオーディオデータである場合に、オーディオデータの前後に販売者や著作権者を示すオーディオデータをマークとして付加し、この付加したマークに第 6 実施形態から第 8 実施形態で埋め込んだ電子透かしを埋め込むようにしてもよい。

【0295】以上、本発明の各実施形態について説明した。

【0296】なお、以上の各実施形態におけるプログラムは、フロッピーディスク、CD-ROM、DVD 等各種記憶媒体に格納された形態で、プログラムを事項する各装置に供給するか、あるいはこれらの装置が接続されたネットワークに接続された他のサーバから当該装置にダウンロードするようにしてもよい。

【0297】また、以上の各実施形態は、その要旨を逸脱しない範囲内で、さまざまに修正することができる。

【0298】

【発明の効果】以上のように、本発明によれば、電子データと個人／機関との関係を、より高い信頼性をもって認証可能とする技術を提供することができる。また、電子データとの関係を認証可能な個人／機関と一致することが保証されるように、電子データと関係を持つ個人／機関を電子データによって利用者に直接提示ことができる。

【図面の簡単な説明】

【図 1】本発明の第 1 実施形態に係るコンテンツ配布システムの構成を示すブロック図である。

【図 2】本発明の第 1 実施形態に係るプロバイダー装置と購入者装置の構成を示すブロック図である。

【図 3】本発明の第 1 実施形態に係る電子計算機の一般

的な構成を示したブロック図である。

【図 4】本発明の第 1 実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図 5】本発明の第 1 実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図 6】本発明の第 1 実施形態に係るコンテンツ配布の処理手順を示したフローチャートである。

【図 7】本発明の第 2 実施形態に係る第 2 配布コンテンツ作成システムの構成を示すブロック図である。

【図 8】本発明の第 2 実施形態に係るプロバイダー装置と権利者装置の構成を示すブロック図である。

【図 9】本発明の第 4 実施形態に係る認証システムの概略構成を示すブロック図である。

【図 10】本発明の第 4 実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図 11】本発明の第 4 実施形態に係る販売者端末のハードウェア構成を示すブロック図である。

【図 12】本発明の第 4 実施形態に係る WWW サーバのハードウェア構成を示すブロック図である。

【図 13】本発明の第 4 実施形態に係る管理サーバのハードウェア構成を示すブロック図である。

【図 14】本発明の第 4 実施形態に係る認証システムの動作を示すフローチャートである。

【図 15】本発明の第 4 実施形態に係るマーク管理 DB の内容を示す図である。

【図 16】本発明の第 5 実施形態に係る認証システムの概略構成を示すブロック図である。

【図 17】本発明の第 5 実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図 18】本発明の第 5 実施形態に係るマーク管理サーバのハードウェア構成を示すブロック図である。

【図 19】本発明の第 5 実施形態に係る認証システムの動作を示すフローチャートである。

【図 20】本発明の第 5 実施形態に係るマーク管理 DB の内容を示す図である。

【図 21】本発明の第 6 実施形態に係るマーク管理サーバの動作を示すフローチャートである。

【図 22】本発明の第 6 実施形態に係る消費者端末の動作を示すフローチャートである。

【図 23】本発明の第 7 実施形態に係るマーク管理サーバの動作を示すフローチャートである。

【図 24】本発明の第 7 実施形態に係る消費者端末の動作を示すフローチャートである。

【図 25】本発明の第 8 実施形態に係る消費者端末のハードウェア構成を示すブロック図である。

【図 26】本発明の第 8 実施形態に係るマーク管理サーバのハードウェア構成を示すブロック図である。

【図 27】本発明の第 8 実施形態に係る販売者端末のハードウェア構成を示すブロック図である。

【図 28】本発明の第 8 実施形態に係るマーク管理サー

バの動作を示すフローチャートである。

【図29】本発明の第8実施形態に係る消費者端末の動作を示すフローチャートである。

【符号の説明】

10 ネットワーク
100 プロバイダ装置

110 処理部

111 入出力部

112 制御部

113 署名抽出部

114 署名検証部

115 暗号化部

116 送受信部

120 記憶部

200 購入者装置

210、710 処理部

211、711 入出力部

212、712 制御部

213、713 送受信部

214、714 復号化部

215、715 署名生成部

216、715 署名埋め込み部

217、717 鍵生成部

220、720 記憶部

1100 (1000-1~1000-n) : 消費者、

1101 (1101-1~1101-n)、1800 (1800-1~1800-n) : 消費者端末、

1102、1301、1401、1501 : 表示装置、

1103 (1103-1~1103-2)、1302、1402、1502 : 入力装置、

1110 : 販売者、

1111 : 販売店、

1112 : 販売者端末、

1113 : WWWサーバ、

1114 : WebページDB、

1120 : マーク管理者、

1121 : マーク管理機関、

1122、1810 : マーク管理サーバ、

1123 : マーク管理DB、

1140 : 通信網、

1200、1300、1400、1500 : バス、

1201、1303、1403、1503 : 通信網インタフェース、

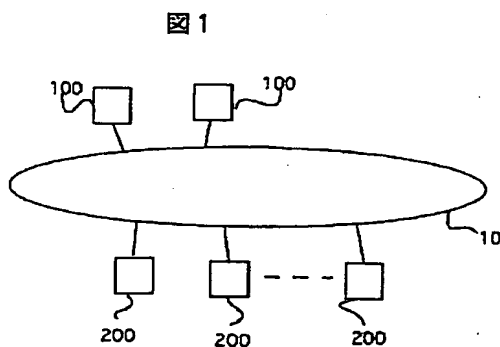
1202、1304、1405、1505 : 記憶装置、

1203、1305、1406、1506 : CPU、

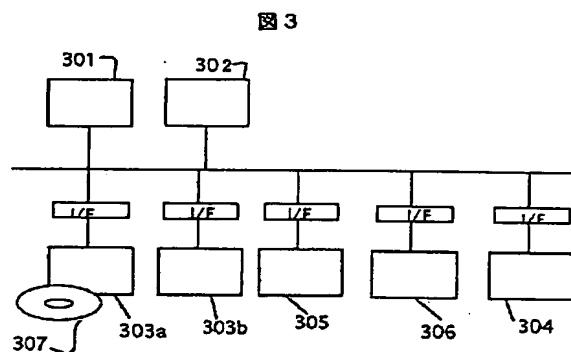
1204、1306、1407、1507、1901、

11000 : メモリ、

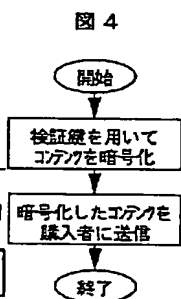
【図1】



【図3】

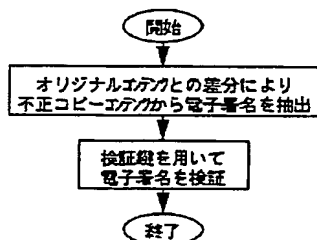


【図4】

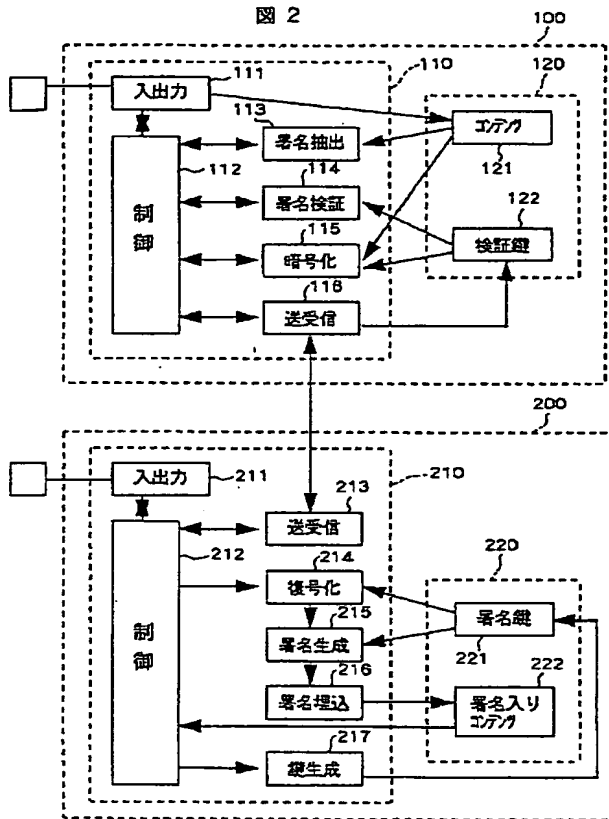


【図6】

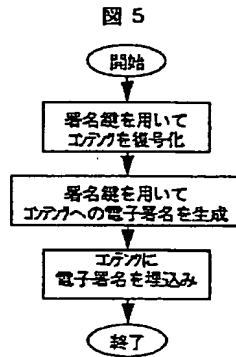
図6



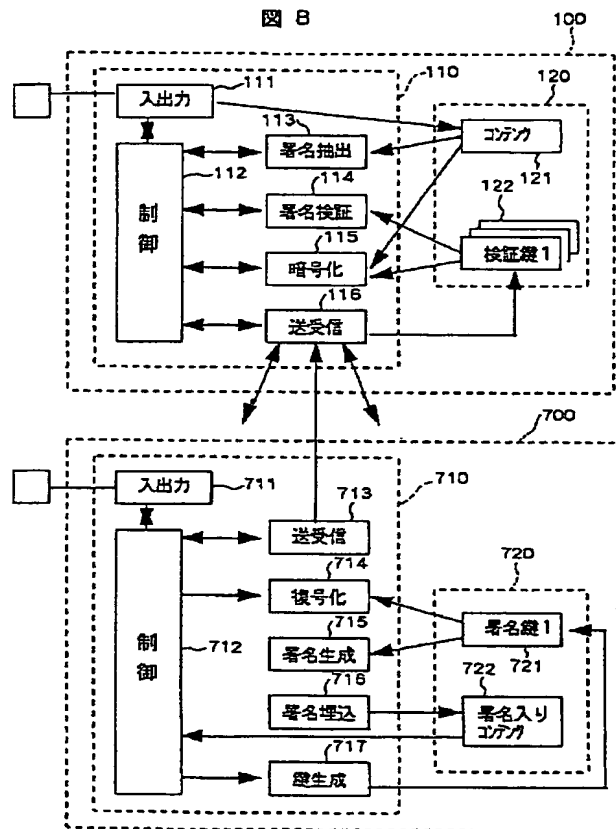
【図 2】



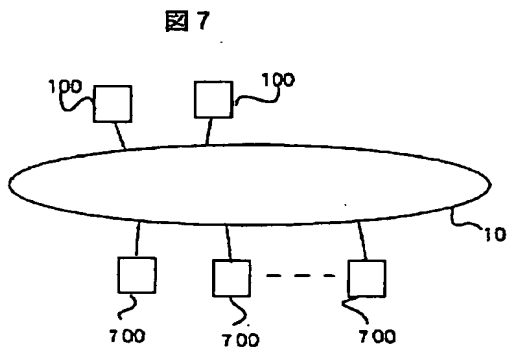
【図 5】



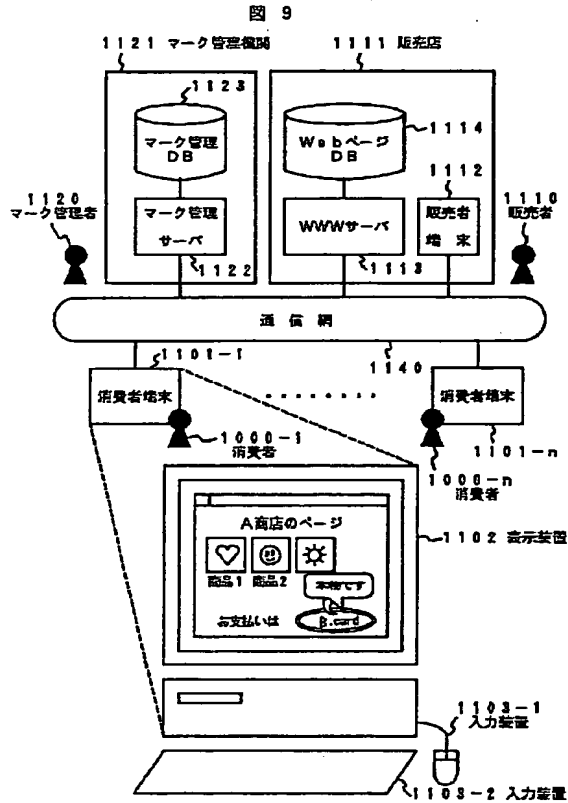
【図 8】



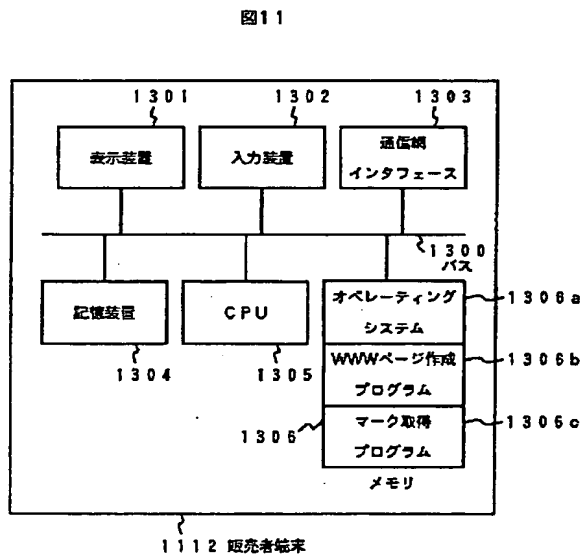
【図 7】



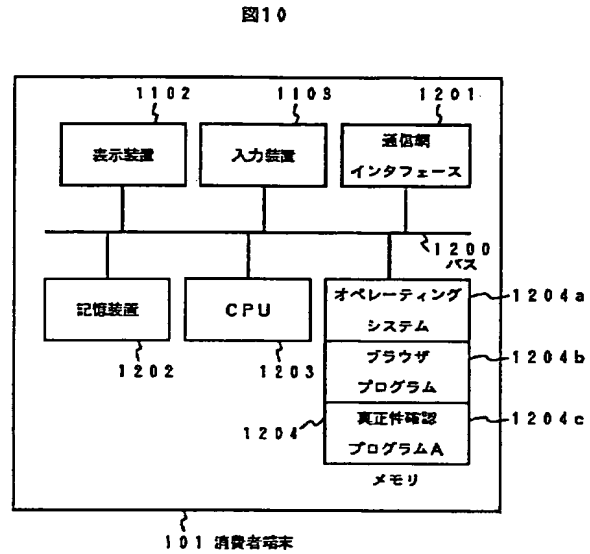
【図 9】



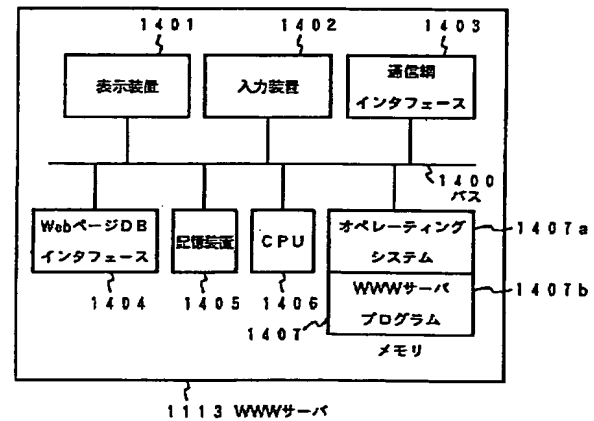
【図 11】



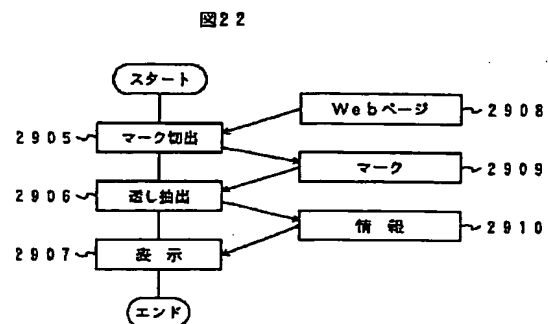
【図 10】



【図 12】

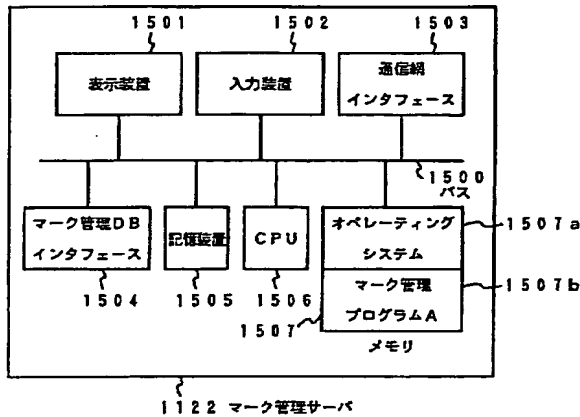


【図 22】



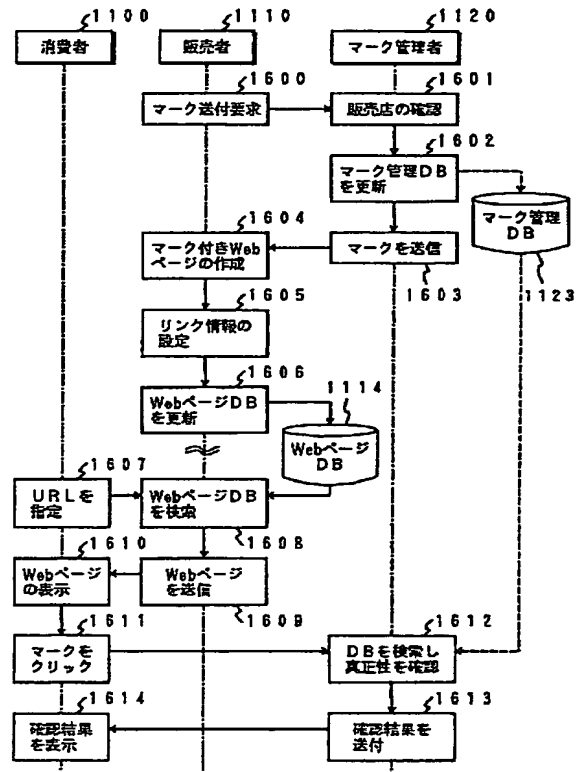
【図13】

図13



【図14】

図14



【図15】

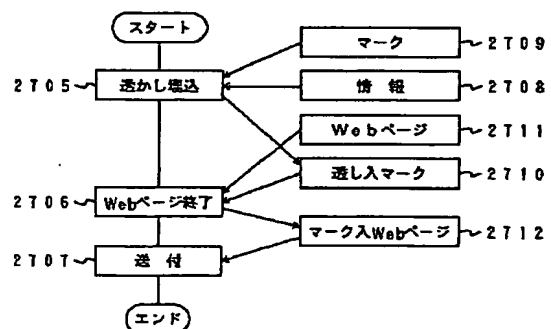
図15

No	日時（有効期限）	マーク種別	販売者	販売店のURL
1	1998. 1. 1～1999. 12. 31	B. Card	A	www. a. co. jp
2	1998. 1. 1～1999. 12. 31	B. Card	C	www. c. co. jp
3	1998. 4. 1～2001. 3. 31	Card. E	A	www. a. co. jp
4	1997. 5. 1～1998. 4. 30	B. Card	D	www. d. co. jp
⋮	⋮	⋮	⋮	⋮

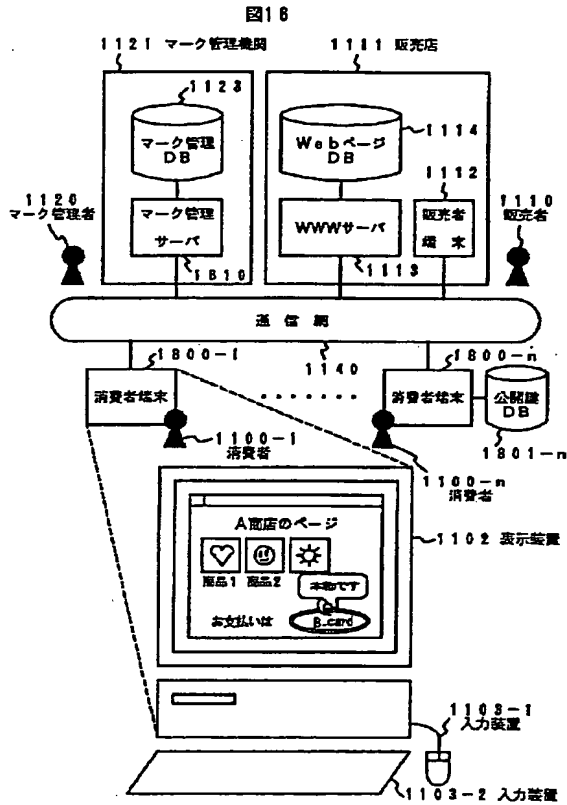
1123 マーク管理DB

【図21】

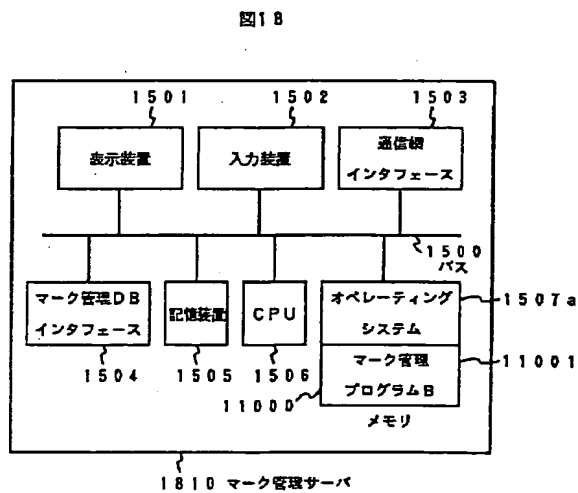
図21



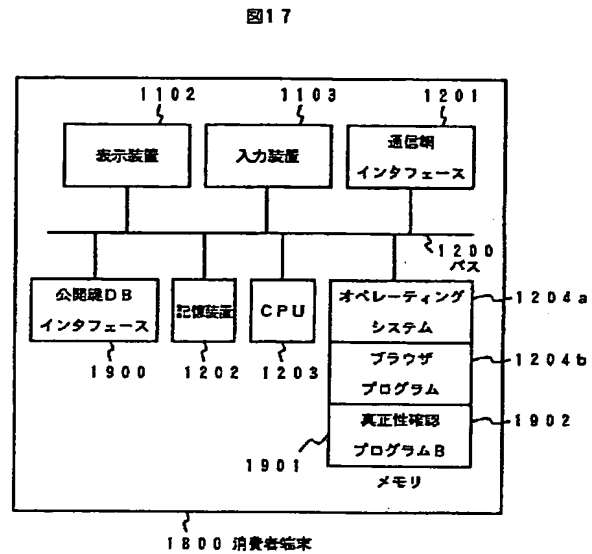
【図16】



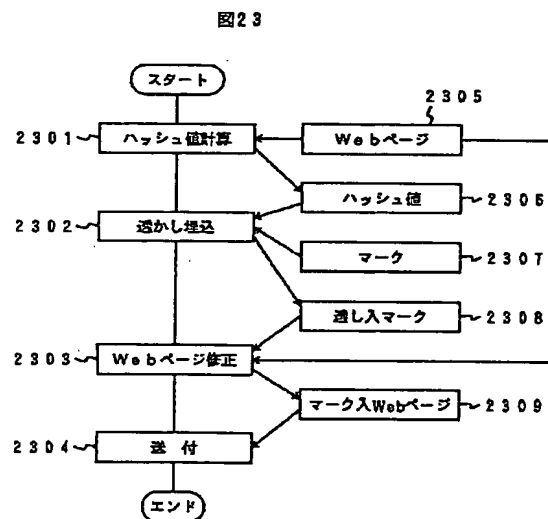
【図18】



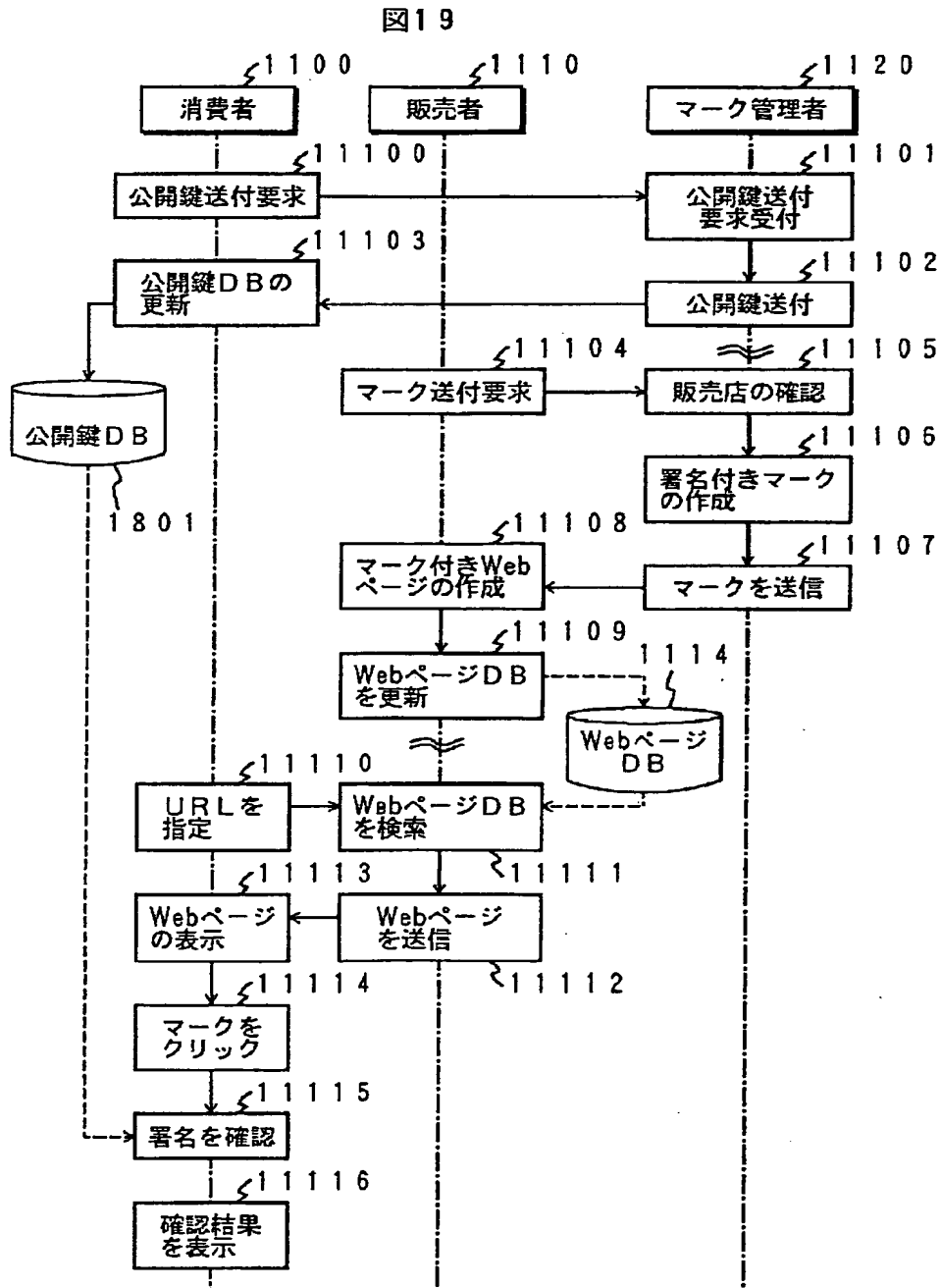
【図17】



【図23】



【図19】



【図 20】

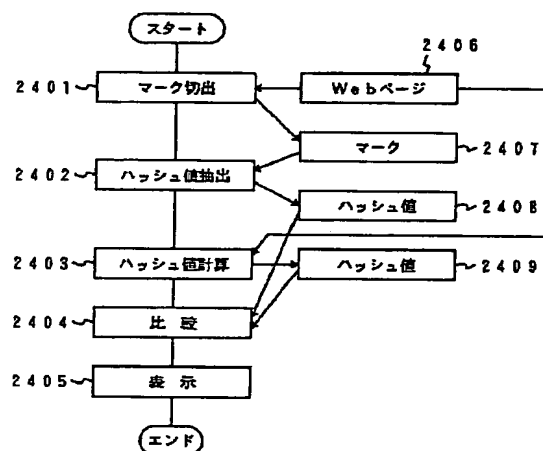
図 20

No	マーク管理者	有効期間	公開鍵
1	α	1997. 1. 1~1998. 12. 31	dayh8u4uf75kweF85p3yd
2	β	1997. 1. 1~1998. 12. 31	gfijvklst867wrf586d84w
3	γ	1997. 4. 1~1999. 3. 31	u57di853riwdyp0895utct
4	δ	1997. 1. 1~1998. 12. 31	ysfywe65uscma3j40abyds
:	:	:	:

1801 公開鍵DB

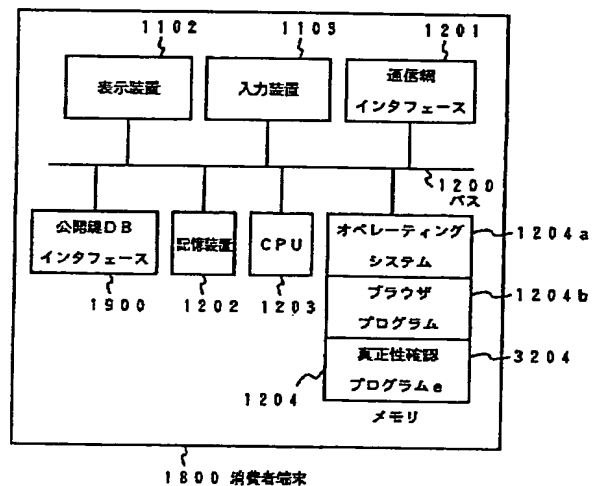
【図 24】

図 24



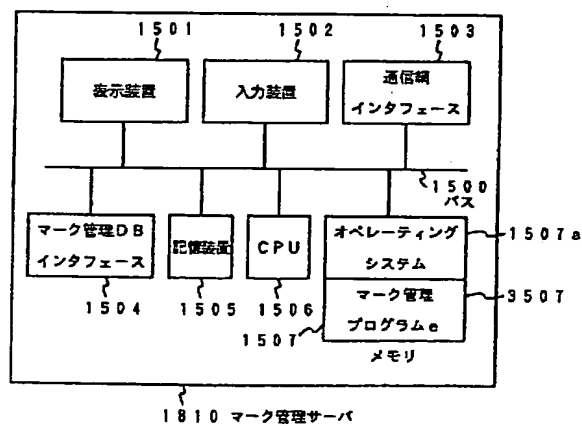
【図 25】

図 25



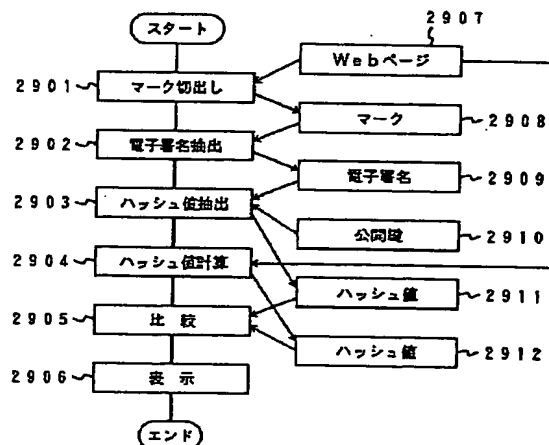
【図 26】

図 26



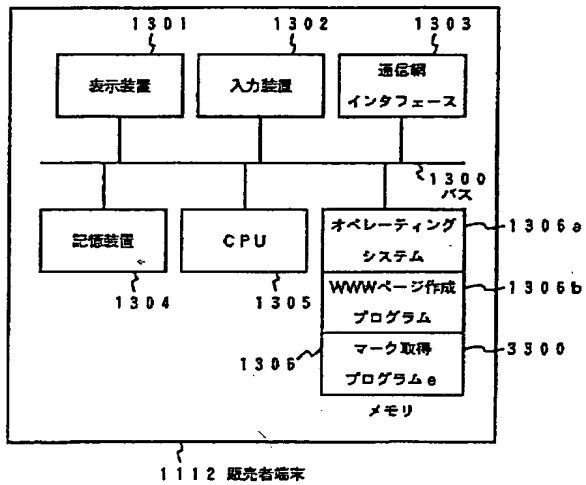
【図 29】

図 29



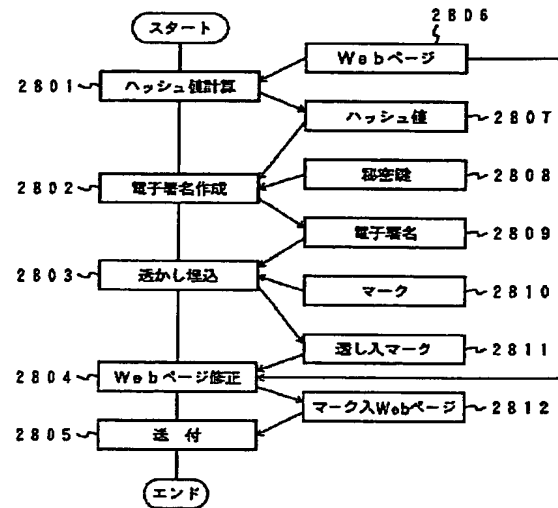
【図 27】

図 27



【図 28】

図 28



フロントページの続き

(51) Int. Cl. 6

識別記号

H 0 4 N 1/387

F 1

H 0 4 N 1/387

(72) 発明者 佐々木 良一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72) 発明者 豊島 久

東京都江島区新砂一丁目6番27号 株式会社日立製作所公共情報事業部内

(72) 発明者 齋藤 司

東京都江島区新砂一丁目6番27号 株式会社日立製作所公共情報事業部内